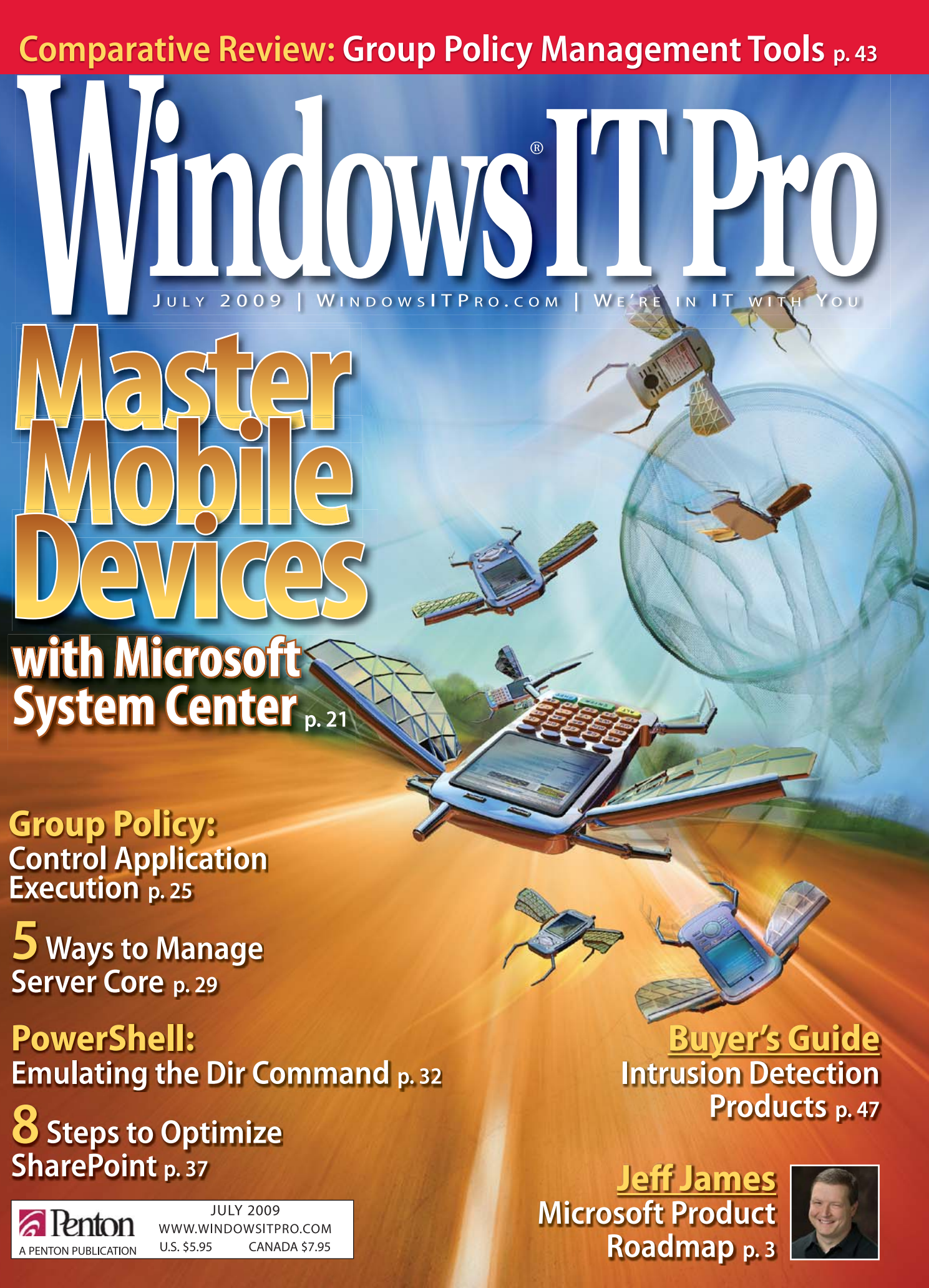
Comparative Review: Group Policy Management Tools p. 43

Windows® IT Pro

JULY 2009 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



Master Mobile Devices with Microsoft System Center p. 21

Group Policy: Control Application Execution p. 25

5 Ways to Manage Server Core p. 29

PowerShell: Emulating the Dir Command p. 32

8 Steps to Optimize SharePoint p. 37

Buyer's Guide Intrusion Detection Products p. 47

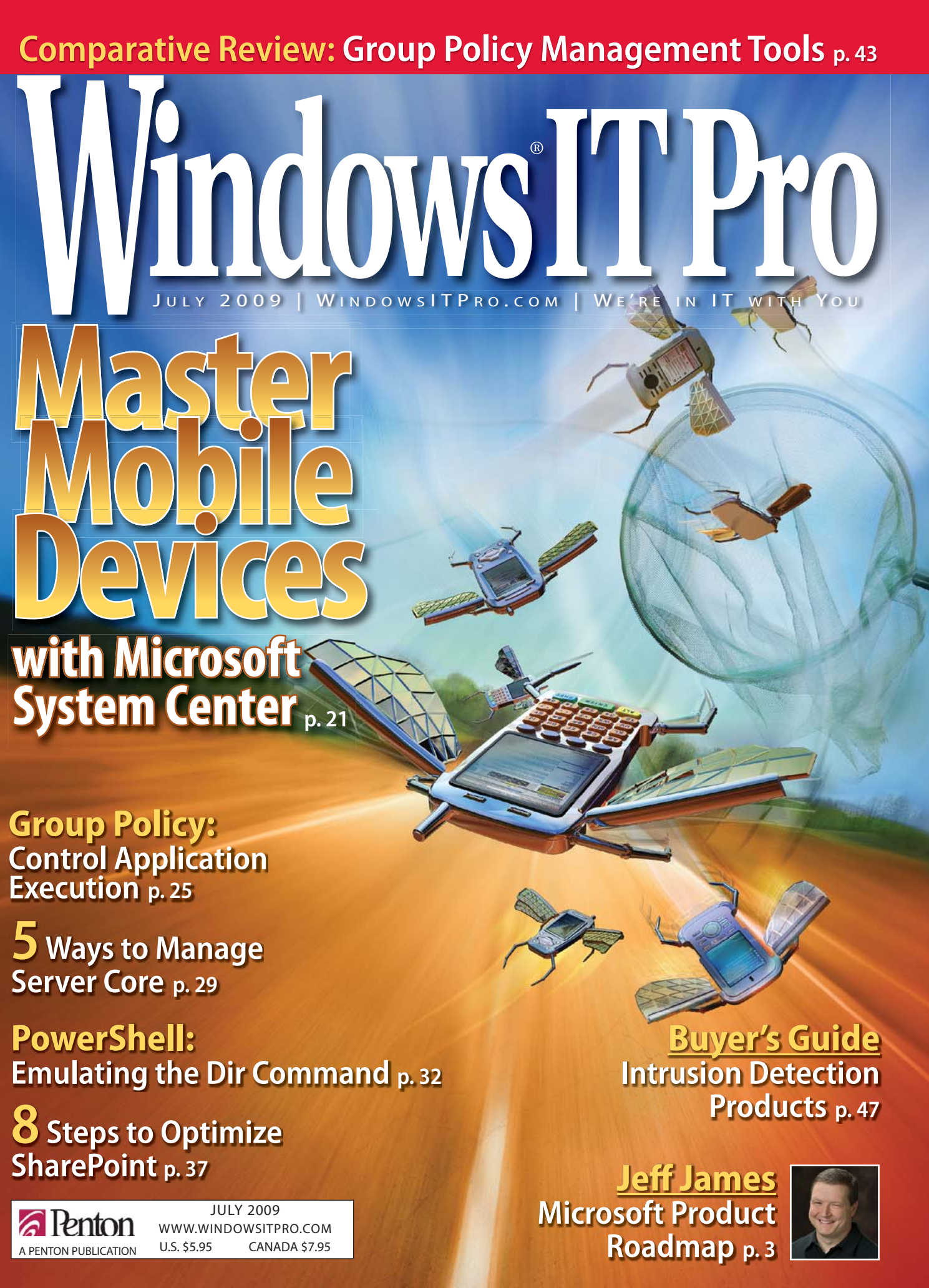
Jeff James Microsoft Product Roadmap p. 3

Penton
A PENTON PUBLICATION
JULY 2009
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

Comparative Review: Group Policy Management Tools p. 43

Windows® IT Pro

JULY 2009 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



Master Mobile Devices with Microsoft System Center p. 21

Group Policy: Control Application Execution p. 25

5 Ways to Manage Server Core p. 29

PowerShell: Emulating the Dir Command p. 32

8 Steps to Optimize SharePoint p. 37

Buyer's Guide Intrusion Detection Products p. 47

Jeff James Microsoft Product Roadmap p. 3

Penton
A PENTON PUBLICATION
JULY 2009
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

Just Released!

BlackBerry Enterprise Server v5.0

Get it now! Free Trial.

Evaluate for yourself how the New BlackBerry® Enterprise Server version 5.0 redefines power and flexibility for IT administrators in your own network environment. Experience how you can do more in less time with a highly efficient upgrade process and centralized administrative controls. See how application management, deployment and user migration have never been easier!

Engineered for mission critical environments, this enterprise-class product provides:

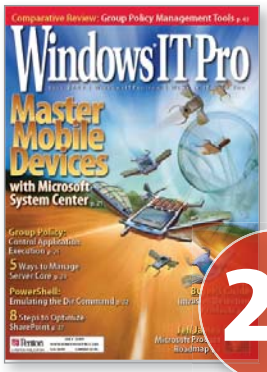
- A built-in high availability architecture
- Powerful, new administrative features
- Enhanced monitoring tools
- Advanced security capabilities
- Improved scalability

Access your free 60-day trial at:
www.blackberry.com/go/ITserver5trial

And if you decide to buy, you'll receive a Free voucher for BlackBerry® Certification Program to get certified as a BlackBerry Certified System Administrator! For more details, visit: *www.blackberry.com/voucherrequest*

BlackBerry®

C O N T E N T S



COVER ILLUSTRATION BY STONEFLYGRAPHICS@GMAIL.COM

COVER STORY

FEATURES

PRODUCTS

INTERACT

Windows IT Pro
A PENTON PUBLICATION

JULY_2009
VOLUME_15
NO_7

COLUMNS

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

CONTENTS

IN EVERY ISSUE

ON THE WEB

Read these articles at www.windowsitpro.com.

Time to Round Up Those Scripts

If you have scripts scattered all over the place on your computer, try ScriptRoundUp.vbs. It locates scripts meeting your criteria, then copies them to a central location so you can back them up and easily find them in the future.

—Jim Turner

InstantDoc ID 102139

Running Exchange 2007 Virtually

Thinking of virtualizing Exchange 2007? Here's what you need to know about storage, sizing, and virtualizing.

—Keith McCall

InstantDoc ID 102150

Windows Gatekeeper

Protect Active Directory objects (like Organizational Units) from accidental deletion by administrators, and find out if you can still terminate the incoming Outlook SSL sessions on your ISA Servers when using SSL and a server publishing rule.

—Jan De Clercq

InstantDoc IDs 102144, 102145

Outlook Tips & Techniques

Learn about the Outlook taskbar shutdown icon in 2007 SP2, find out what the Outlook Mobile Service account is, and disable that annoying telephony service pop-up window that shows up in Outlook if you have Vista.

—William Lefkovics

InstantDocs ID 102159, 102160, 102161

New Ways to Reach *Windows IT Pro* Editors

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director
Michele Crockett mcrockett@windowsitpro.com

Editor-in-Chief, Web Content Strategist
Jeff James jjames@windowsitpro.com

Executive Editor, IT Group
Amy Eisenberg amy@windowsitpro.com

Technical Director
Michael Otey motey@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Web and Developer Strategic Editor
Anne Grubb agrubb@windowsitpro.com

Systems Management
Karen Bemowski kbemowski@windowsitpro.com
Caroline Marwitz cmarwitz@windowsitpro.com
Zac Wiggy zwiggy@windowsitpro.com

Messaging , Mobility, SharePoint, and Office
Brian Keith Winstead bwinstead@windowsitpro.com

Networking and Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security
Lavon Peters lpeters@windowsitpro.com

SQL Server
Megan Bearly Keller mkeller@windowsitpro.com
Sheila Molnar smolnar@windowsitpro.com

Production Editor
Brian Reinholz breinholz@windowsitpro.com

IT Media Group Editors
Linda Harty, Chris Maxcer, Rita-Lyn Sanders

CONTRIBUTORS

News Editor
Paul Thurrott news@windowsitpro.com

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond tony.redmond@hp.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
John Savill john@savilltech.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Senior Art Director
Larry Purvis lpurvis@windowsitpro.com

Art Director
Layne Petersen layne@windowsitpro.com

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Production Manager
Kate Brown kbrown@windowsitpro.com

Assistant Production Manager
Erik Lodermeier erik.lodermeier@penton.com

ADVERTISING SALES

Publisher Peg Miller pmiller@windowsitpro.com

EMEA Managing Director Irene Clapham irene.clapham@penton.com

Director of Sales Birdie J. Ghiglione birdie.ghiglione@penton.com, 619-442-4064

Online Sales and Marketing Manager Dina Baird Dina.Baird@penton.com

Key Account Directors
Jeff Carnes jeff.carnes@penton.com 678-455-6146
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883
Jacquelyn Baillie jacquelyn.baillie@penton.com 714-623-5007

Account Executives
Barbara Ritter barbara.ritter@penton.com 858-759-3377
Cass Schulz cassandra.schulz@penton.com 858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service 800-793-5697 (US and Canada) 44-161-929-2800 (Europe)

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

Penton
Penton Media, Inc.

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com

Chief Financial Officer/Executive Vice President
Jean Clifton jean.clifton@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS

Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

REPRINTS

Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

James

"Microsoft is gearing up for a significant product launch period."

Upcoming Microsoft Releases

Are you ready for the product onslaught?

Judging by the announcements Microsoft made at TechEd 2009, the company is gearing up for a significant product launch period, with close to a dozen major product releases between the last half of 2009 and the end of 2010. Here's a sample of Microsoft's upcoming product portfolio, along with *Windows IT Pro* articles about these products.

Windows 7 (ETA: Dec 2009)—By nearly all accounts, Windows 7 is shaping up to be a significant improvement over Windows Vista. Granted, one could argue that Windows 7 has more in common with Vista than Microsoft would care to admit, but the OS offers important UI and performance enhancements. Although many IT administrators decided to pass on Vista, I have a feeling Windows 7 adoption will be robust. (Windows 7 FAQ, winsupersite.com/win7/faq.asp)

Exchange 2010 (ETA: H2 2009)—Microsoft Exchange 2007 is powerful, but it can be overly complex to manage. Microsoft hopes to address some of that complexity in Exchange 2010, as well as mix in some new features to tackle security and e-discovery. The 2010 version of Outlook Web Access also looks impressive, with a feature set that nearly matches the traditional Outlook client. ("A First Look at Exchange 2010," windowsitpro.com/article/articleid/100934)

Windows Server 2008 R2 (ETA: H2 2009)—Some Microsoft execs I've spoken to have attempted to minimize the importance of VMware's vMotion technology, but IT pros using VMware tell me that it's a critical feature. (VMware vMotion lets you move and copy virtual machines without turning them off.) Server 2008 R2 will ship with a comparable feature dubbed Live Migration, which could help Microsoft gain some ground against VMware in the still-booming virtualization market. ("Inside Windows Server 2008 R2," windowsitpro.com/article/articleid/101706)

Office 2010 (ETA: H1 2010)—The Office family of products has been a cash cow for Microsoft over the years, but this product suite is now in an increasingly competitive fight on the low end of the market with SaaS Office work-alikes such as Google Docs, Zoho Office, and ThinkFree Office. Can Microsoft's leading app suite fend off competitors while keeping large enterprise admins happy? ("Office 2010 Details Emerge," windowsitpro.com/article/articleid/102140)

SharePoint Server 2010 (ETA: H1 2010)—I wrote about the exploding SharePoint market last month; SharePoint Server 2010 looks to continue Microsoft's SharePoint hot streak. Some early system requirements: SharePoint Server 2010 will be 64-bit only and will require a 64-bit version of SQL Server 2008 or SQL Server 2005 and the 64-bit version of Server 2008 or Server 2008 R2. ("SharePoint 2010 Features, System Requirements Emerge," windowsitpro.com/article/articleid/102113)

SQL Server 2008 R2 (ETA: H1 2010)—The latest version of SQL Server 2008 will offer a host of upgrades and feature improvements, including support for up to 256 logical processors; a new "Self-Service BI" feature that integrates BI reporting through SharePoint, Excel, and SQL Server; and the inclusion of Master Data Services, a new feature that streamlines and improves the management of data across multiple data sources. SQL Server has steadily been making inroads into enterprises that historically would have been the provinces of IBM and Oracle, and SQL Server 2008 R2 should help continue that trend. ("More SQL Server 2008 R2 News," sqlmag.com/article/articleid/102112)

Windows Mobile 7 (ETA: H1 2010)—Microsoft was caught flat-footed by Apple's iPhone and RIM's latest Blackberry devices, and the company is also trailing in the development and launch of its answer to Apple's popular iPhone App Store. The recently launched Windows Mobile 6.5 offers some needed improvements to Microsoft's mobile UI, but Microsoft definitely has a big hill to climb in this category. Microsoft hasn't confirmed yet if Windows Mobile 7 will be an actual product name; regardless, whatever succeeds WinMo 6.5 has a lot of catch-up work to do. ("Windows Mobile Update in Late 2009," windowsitpro.com/article/articleid/101258)

Microsoft's upcoming product launch schedule is undoubtedly impressive, but it also raises some questions. Given the depressed economy and shriveled IT budgets, few IT departments are likely to have the financial resources to deploy all of these product upgrades. What do you think? Are some of these upgrades more attractive than others? And will Windows 7 convince you to leave XP behind?

InstantDoc ID 102191

Talk Back: Tell Us What You Think

We're always eager to hear reader feedback on everything we do here at *Windows IT Pro*, so I encourage you to let us know what's on your mind. Drop me an email at jjames@windowsitpro.com, follow me on Twitter (twitter.com/jeffjames3), or give me a call directly at 970-203-2775. We also invite you to participate in an online survey about Microsoft's upcoming products, which you can access at http://tinyurl.com/p85xzs.

JEFF JAMES (jjames@windowsitpro.com) is Editor-in-Chief, Web Content Strategist for Penton Media's IT Publishing Group. He specializes in server operating systems, systems management, and server virtualization.

- Printer Mapping
- Windows 7
- Storm Weathering
- SBS Counterpoint

LETTERS@WINDOWSITPRO.COM

Updated Code for Mapping Printers

We've extended the support code for "Create Site-Specific Printer Mappings for Mobile Users" (March 2009, InstantDoc ID 101230) to work around two specific problems: IP4 addresses assigned to disconnected adapters and automatic IPv6 addresses generated for Windows Vista and later systems. Thanks to Roy Ulrick and Stuart Cleveland for providing feedback and testing!

—Alex Angelopoulos

Streamlined Windows 7

One of the exciting benefits of Windows 7 is that it supposedly requires less hardware than Windows Vista does. I'm excited to try it out on one of my older laptops, which is currently running Windows XP. However, the laptop doesn't have a DVD drive, and so far I've seen only DVD images of the Windows 7 beta releases. Do you know how to obtain CD images from the DVDs?

—Ze'ev Ionis

I'm not aware of any CD media for Windows 7. But you can pick up an inexpensive USB DVD drive that you can boot from. Or, you can create a bootable USB stick with Windows 7 on it and install from there. You could even use Windows Server 2008 R2 Windows Deployment Services and allow the installation over the network. But the easiest solution would be to buy a USB DVD drive. Windows 7 is based on a single Windows Imaging Format (WIM) file that's over 2GB in size. You would have to split the WIM file to put it on a CD.

—John Savill

Weathering the Storm

Recently, I've noticed that *Windows IT Pro* isn't as thick as it once was, and so I considered canceling my subscription. Then, I read Michele Crockett's IT Pro Perspective column, "Riding Out the IT Storm" (April 2009, InstantDoc ID 101536). After reading her article, I've decided to continue subscribing as I have since 1997.

I understand the cost factor, and I believe things will turn around for IT. In the publishing world, online content is the new way for people to get their information. I would suggest that you create a mobile website so that readers can get content on their mobile devices.

We have to support one another through the good times and the bad. So, I'm sticking it out with you guys. I'll check out the resources on the web that Michele mentions, and I'll also download Paul Thurrott's Windows Weekly podcast (www.winsupersite.com/paul/podcast.asp) to get my timely Microsoft information—as well as some Mac bashing! Anyway, please continue to help us IT folks stay informed and educated about the latest technologies.

—Gary Godfrey

SBS Best Practices: A Matter of Perspective

I was disappointed to read Mike Zylberstein's letter in your April issue (InstantDoc ID 101570). Mike, please stop undoing what you call "SBS wizardry." Microsoft has provided those Small Business Server (SBS) features for good reasons—not least of which because we requested them!

I often have to inspect or repair SBS systems built by people who insist on undoing SBS's default settings. Why would someone want to alter settings created, tested, and approved by the SBS Dev team, hundreds of beta testers, and the great majority of SBS implementers? Please stop disabling those features! When your client calls me, I'll just have to charge them to reinstate the original settings.

—Mick Malloy, SBS MVP

InstantDoc ID 102158

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

ONLINE

windowsitpro.com

Battery Drain?

John Savill's answer to the question, "What uses the most battery power on my laptop?" (April 3, 2009, www.windowsitpro.com, InstantDoc ID 101790), is helpful, but I have another question. I've heard that wireless networking consumes battery power like crazy, and that's the reason most current laptops tend to shut down the radio when it's not in use. Is this true? Is that aspect factored into John's "Network" result of 4 percent? I would expect this result to be much higher if wireless networking is truly a concern.

—Phil Powers

Interesting question. I did some additional research and found that most modern wireless and Bluetooth networks aren't the huge battery killers we typically think they are, compared with something like a large laptop screen. The 4 percent figure includes wireless and Bluetooth. Yes, it's great to turn those radios off if you aren't using them. However, consider the average mobile phone and its tiny battery. Those devices have WLAN/Bluetooth, and they can run for an entire day. Now, consider the battery inside a laptop. The proportion of battery used by WLAN/Bluetooth is comparably small. That being said, turning off the network is also a good idea from a security perspective: You don't want to advertise the availability of networks that you're not even using.

—John Savill

Humphries

The missing link to IT resources

ONLINE

windowsitpro.com

Unisys Offers a New Platform for SQL Server Scalability

Looking for the best platform for SQL Server databases? Read this WinterCorp report on the new, top-of-the-line Unisys ES7000 Server. Learn more about how it delivers distinctive capabilities for users with rapidly growing database requirements on SQL Server, and why it received high marks in performance and scalability.

windowsitpro.com/go/SQLScalabilityReport

Find the Right Search Solution for Your Business

Any company or organization in the process of deploying search or in the planning phases, will at one time or another hear users ask, "Why can't it just be like Google?" Microsoft has been trying to develop a unified search strategy, which requires rationalizing its disparate search portfolio. That process is still unfolding, so the company now has three products capable of meeting various search needs. Listen to this podcast to explore the search solutions available to determine the right search solution for your business!

windowsitpro.com/go/SearchSolutions

Hyper-V Unleashed - LIVE Online Event: July 21, 2009

Join experts Michael Otey, John Savill, and Michael K. Campbell to find out how Hyper-V stacks up against ESX Server, how to best manage Hyper-V, how to set up Failover Clustering for Hyper-V, and much more! During the event, you'll get to meet premier virtualization technology vendors as they demonstrate, showcase, and exhibit their virtualization products and services, including VMware and Microsoft Windows Server 2008 Virtual Machine solutions. PLUS don't miss your chance to win an iPod nano!

windowsitpro.com/go/Hyper-VUnleashed

Flip Your Script

Check out these *Windows IT Pro* resources to give your scripting skill set a boost

There's nothing I like better than a "flipped script." I'm good—actually great—at figuring out what is going to happen. I can read the clues in social situations, usually figure out what our organization's corporate office will do next, and even deduce the ending of most any movie. So when someone comes along and surprises me, I have all that much more respect for them. And in a tough job market where you have to show that not only can you do the tasks you're hired for but also anything else the company throws at you, it helps to have some surprise skills up your sleeve. Make sure your abilities don't get pegged for less than they are: boost your skills with my favorite scripting resources:

"Active Directory Growth Tracker: A Script to Count Objects," InstantDoc ID 101930: Keep an eye on specific AD areas for planning and forecasting with this script.

"Utility Can Help Reduce UAC Headaches When Working with Scripts," InstantDoc ID 101460: Run .vbs and .js scripts under administrative privileges with just a few clicks.

"Scripting on a Cluster," InstantDoc ID 101466: Find out what happens as Jim Turner works to avoid long run time and network traffic by running a .cmd script locally on each cluster node.

"Features of PowerGUI Script Editor," InstantDoc ID 100758: Learn how to put a GUI face on your Windows PowerShell scripting, plus what Michael Otey loves best about the tool, with his Top 10.

"Scripting Utilities to Keep Tabs on Your Printers," InstantDoc ID 101483: Keep an information history on your printers and track changes to help troubleshoot with these two scripts.

"Moving from Command Shell Scripting to PowerShell," InstantDoc ID 100796: Michael Otey shares his experience and learning curve when shifting to PowerShell.

"Free Utility Lets You Retrieve a Little or a Lot of Inventory Information," InstantDoc ID 100461: Get through an inventory task just how you need to with this utility.

"Create Site-Specific Printer Mappings for Mobile Users," InstantDoc ID 101230: When used with an existing network logon script, this script automatically determines which site a mobile user is in, then maps the appropriate printers at that site.

PowerShell 101 and 201 eLearning series: Get the lowdown on PowerShell with Paul Robichaux's online eLearning series about PowerShell basics—available on demand at windowsitpro.com/go/PowerShell101 and windowsitpro.com/go/PowerShell201.

***asp.netPRO* magazine:** If your interest lies in ASP.NET code, check out our newest addition to the *Windows IT Pro* family—complete with ready-to-run code and pages—at aspnetpro.net!

To step outside your comfort zone and into your can-do zone, check out other hot topics that aren't your specialty and beginner how-tos on windowsitpro.com. Who knows? You might just surprise yourself.

InstantDoc ID 102095

ALTERNATIVE THINKING ABOUT SERVER ECONOMICS:

Perform like a superstar. Save like an accountant.

Now more than ever, you need your money to work harder. With the new generation of HP ProLiant G6 Servers with Intel® Xeon® processor 5500 series you dramatically improve energy efficiency, flexibility and performance. And more reliability in each system means you can reduce business risk as you increase your productivity.

Decrease your IT support costs to an absolute minimum. HP Insight Control Suite (ICE) will help you to reduce operational expenses by up to $48,380 per 100 users.*

For total peace of mind, HP Care Pack Services deliver industry leading automated 24X7 system monitoring, diagnosis and fault notification to protect your investment.

Making you and your business shine.

Technology for better business outcomes.

HP ProLiant DL360 G6 Server
- Up to two Intel® Xeon® Processor 5500 Series
- 144 GB maximum memory footprint
- Supports up to 8 small form factor high-performance SAS hard drives
- HP ProLiant Onboard Administrator powered by Integrated Lights-Out 2

$2,969 (Save $723)
Lease for just $72/mo.**
Smart Buy [PN:519567-005]

HP ProLiant BL460c G6 Server Blade
- Up to two Intel® Xeon® Processor 5500 Series
- 96 GB maximum memory footprint
- Embedded Dual Port Flex-10 10GbE Multifunction Server Adapter
- HP ProLiant Onboard Administrator powered by Integrated Lights-Out 2

$2,209 (Save $375)
Lease for just $54/mo.**
Smart Buy [PN:532020-B21]

HP BladeSystem c3000 Enclosure
- Supports up to 8 server/storage blade devices in a 6U enclosure
- Optional HP Insight Control Environment management suite
- Low-line or high-line power options for maximum power flexibility

$3,499 (Save $2,319)
Lease for just $85/mo.**
Smart Buy [PN:481657-001]

Special 0% financing for up to 36 months also available.†
To learn more, call 1-866-625-1012 or visit hp.com/go/G6superstar11

*Source: IDC white Paper sponsored by HP, "Gaining Business Value and ROI with HP Insight Control" Document #210479, Feb 2008. **Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount and are good while supplies last. All featured offers available in U.S. only. Savings based on HP published list price of configure-to-order equivalent (Enclosure: $5,818–$2,319 instant savings = SmartBuy price of $3,499; BL Server: $2,584–$375 instant savings = SmartBuy price of $2,209; DL Server: $3,692–$723 instant savings = SmartBuy price of $2,969. Financing available through Hewlett-Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the U.S. and is subject to credit approval and execution of standard HPFSC documentation. Prices shown are based on a lease 48 months in term with a fair market value purchase option at the end of the term and are valid through July 31, 2009. Other rates apply for other terms and transaction sizes. Financing is available on transactions greater than $349. Other charges and restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice. †Financing available through Hewlett Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the US and Canada and is subject to credit approval and execution of standard HPFSC documentation. Offer valid through July 31, 2009 on transactions in the United States between $1,500 and $150,000 USD and in Canada between $5,000 CAD and $150,000 CAD. Zero percent financing assumes transaction is documented as a lease with a $1 end-of-term purchase option (or local country equivalent), assuming lessee is not required to pay any nominal end-of-term purchase price at the end of the lease term and disregarding any changes payable by lessee other than rent payments such as maintenance, taxes, fees and shipping. This offer cannot be combined with any other rebate, discount or promotion without prior approval by HP and HPFSC. Rates are based on customer's credit rating, financing terms, offering types, equipment type and options. Not all HP products are eligible for the 0% lease rate. Not all customers may qualify for these rates. Other restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

Thurrott

"R2 is a seemingly minor update that adds almost as much new functionality as its predecessor."

What You Need to Know About Windows Server 2008 R2 RC

Windows Server 2008 R2 RC is a signal from Microsoft that Server 2008 R2 has hit the home stretch. "It's time to kick tires and evaluate it," Microsoft group product manager Ward Ralston told me during a recent briefing. Microsoft is ready to talk performance, and although the number of performance comparisons I was shown is small, more are on the way. Here's what you need to know about Windows Server 2008 R2 RC.

What's New in the RC

Server 2008 R2 is an ambitious release that dramatically increases the capabilities of the Windows Server lineup. Server 2008 R2 RC includes many new features worth examining.

File Classification Infrastructure. FCI provides an infrastructure for classifying business data by using file labels and properties and gives you the ability to apply policy based on that classification. FCI is managed via the File System Resource Manager (FSRM) and is compatible with Microsoft's SharePoint technology. You can create rules that move or delete files on a schedule-based basis or use other criteria. It's also extensible by third parties.

Hyper-V improvements. As you might recall, Microsoft shipped Server 2008 with a prerelease version of its virtualization technology and delivered Hyper-V 1.0 later in 2008. (Hyper-V 1.0 is included with Server 2008 SP2, shipped to customers in May.) In RC, Hyper-V 2.0's long-awaited Live Migration feature includes a processor compatibility mode. Previously, you could perform Live Migration only between servers that were running the same processor family and version (i.e., if one server was running on Intel Core 2 Duo, the other also needed to be running on Intel Core 2 Duo). Now, you can perform Live Migration between servers of the same processor family. Microsoft says it's working to add cross-migration between AMD-and Intel-based servers in a future release.

A new Hyper-V feature called VM Chimney provides TCP offload support to VMs, letting you map a VM to a physical NIC on the host computer and bypass the virtual interface, improving performance. Although disabled by default, in scenarios such as Microsoft SQL Server backup and restore and Live Migration, VM Chimney provides dramatic improvements, Microsoft says.

Microsoft also added Virtual Machine Queue (VMQ) functionality to RC. It, too, is disabled by default because only Intel currently makes VMQ-enabled hardware; Qualcomm has announced it's entering this market. With VMQ, you can create a unique virtual network queue and pass network packets from the hypervisor to the VM.

Performance and Scalability Improvements

R2 supports more logical processors—now 256. But it isn't enough to just support processors arbitrarily, Bill Karagounis, the principal group program manager of the Windows Server business group, told me. "We did work around NUMA enhancements, so we're well aware of the underlying hardware and topology of that hardware. This is a critical enhancement for scalability."

I was interested to hear Microsoft's first public revelations about the scaling improvements in R2, which experiences near-linear (1.7 times) scaling when moving from 64 processors to 128 on an OLTP SQL Server workload. And throughput on the FSCT file server workload capacity test improves 32 percent from Server 2008 against R2. (This required Microsoft engineers to change code from the days of NT creator David Cutler. "That was his code," Karagounis said, "and let's just say he paid very close attention to the changes we made.")

Karagounis noted that some of these changes were also backported to Server 2008 SP2, so existing customers can see these improvements by updating to SP2. Note, too, that R2 is 64-bit only.

Timing and Availability

Looking ahead, Microsoft's Ralston confirmed that both Windows 7 and R2 would ship by the end of 2009, and not in 2010 as had been widely reported. "As you suspect, Windows Server 2008 R2 will come out in the second half of this year," Ralston told me. "We'll have more details to discuss as time goes by, but you can expect the RTM and launch in the next couple of months." Microsoft projects the next Windows Server release will occur in 2012.

Final Thoughts

R2 is a seemingly minor update that, in fact, adds almost as much new functionality as its predecessor. For businesses using Microsoft's volume licensing scheme, R2 comes with the package, so look at it closely, especially for your machines that provide virtualization functionality. That said, Server 2008 R2 might be less compatible with software designed for the previous Server version than a typical R2 release. For this reason, it will require additional testing, but the sheer amount of new functionality in Server 2008 R2 RC marks this release as a major update worth examining.

InstantDoc ID 102066

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"Is Powercfg still useful in the age of Windows Vista? Sure it is!"

Powercfg Revisited

Control Windows Vista power settings from the command line

Powercfg.exe, a tool built into Windows XP SP2 that lets you manage power configuration from the command line, has two strengths over the Power Options GUI: You can use it to broadcast a given set of power-management settings to a large number of systems, and you can use it to control XP's screen-dimming capability.

Since I introduced the tool in "Powercfg" (January 2006, InstantDoc ID 48399), Windows Vista has appeared, and the newer OS not only includes power-management control through Group Policy, but the Power Options GUI lets you control when your system dims your screen. Is Powercfg still useful in the age of Vista? Sure it is! First, I still often need to tweak or interrogate the system about certain power settings from the command line. And second—at least in my case—Powercfg helped me solve a laptop mystery.

I do much of my Vista and Windows 7 testing on an inexpensive, no-name laptop, and I like it quite a bit except for one thing: If I put the laptop to sleep and awaken it later, its Ethernet port no longer works. The power LED still lights and the activity LED still flickers, but nary a byte seems to pass through the port, either coming or going. Everything else works fine after waking from sleep, but the necessity to reboot to get my wired Ethernet connection back is a pain.

I thought I'd just gotten a system with a bad Ethernet chip until I ran across the Powercfg -devicequery command. From an elevated command prompt, I typed

```
powercfg -devicequery wake_from_any
```

This command inventories the system's hardware and shows what devices are capable of going to sleep and coming back. Guess which component wasn't on the list? If you find that some part of your computer isn't on the list, don't despair: As I understand it, the question of whether something can sleep is typically a question of whether the manufacturer has written a decent driver for it rather than an evaluation of the hardware itself.

The Vista/Windows Server 2008 Powercfg is more useful overall than XP's version, but one aspect could be better: It's obsessed with GUIDs rather than friendly names for power schemes and settings. For example, suppose you've found (as I have) that working with virtual machines (VMs) in the *Power saver* power-management setting is a bad idea—the VMs seem to lock up for some reason. You want to delete the scheme altogether. You'd love to just type

```
powercfg -delete "power saver"
```

but you can't. Instead, you'd need to type

```
powercfg -delete a1841308-3541-4fab-bc81-f71556f20b4a
```

As you've probably guessed, that a1841308-3541-4fab-bc81-f71556f20b4a is the the GUID of the *Power saver* scheme. Note that Powercfg is probably the only Windows utility that works with GUIDs but doesn't need the curly braces around it.

For a listing of your power schemes and their GUIDs, type

```
powercfg -l
```

That's a lowercase L, not the number 1. You'll find that these GUIDs seem to be uniform across the Windows platform. Once you know how to get a power scheme's GUID, you can easily understand a bunch of Powercfg options. You're already familiar with the delete (-d) option. With the -setactive option, you can switch your system to a particular power option. For example, the command

```
powercfg -setactive 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c
```

sets your system to use the *High performance* power scheme. You can discover your system's current power scheme by typing

```
powercfg -getactivescheme
```

If you want to create a new scheme of your own, you'll find -duplicatescheme and -changename useful. For example, if I want to create a new power scheme that's simply a variant of the *High performance* scheme, I'd type

```
powercfg -duplicatescheme 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c

Power Scheme GUID: 77d5b6b8-ea68-4a1f-84e3-71e001ebc159
  (High performance)
```

The response from the system tells me the GUID of the new scheme and the name, which is still *High performance*. Having two schemes with the same name would be a bit confusing, so I could then change the name, as follows:

```
powercfg -changename 77d5b6b8-ea68-4a1f-84e3-71e001ebc159
  "Modified high performance"
```

That's not all Powercfg can do. Check back next month for more!

InstantDoc ID 102005

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books.

Otey

"Without a doubt, the most important missing feature is built-in support for virtualization."

FAQs about Windows Server 2008 Foundation

Get rolling with AD, DNS, and other network services for small businesses

Microsoft is typically fairly predictable, but sometimes the company is able to pull a few surprises out of the old hat. One of those surprises was the April 1 announcement of Windows Server 2008 Foundation. And despite the date of the announcement, this product is no joke. You can find all the details on Microsoft's website at microsoft.com/windowsfoundationserver. In this column I'll address some of the top questions about this new member of the Windows Server family.

1 **Is Windows Server 2008 Foundation part of the Windows Small Business Server (SBS) family?**—No, it's part of the Windows Server 2008 product line. Windows Server Foundation doesn't include integrated email and other services, as SBS does. Instead, it provides basic network infrastructure services.

2 **Isn't this just a version of Windows Server designed to compete with Linux?**—Not really. Although Windows Server Foundation provides an alternative to Linux servers, it's primarily designed as a low-cost option for small businesses that don't already have a server.

3 **Is Windows Server Foundation basically the same thing as Windows Home Server?**—No. Windows Home Server isn't licensed for business use, and although it possesses a nice integrated backup component, it can't act as an Active Directory (AD) domain controller. Windows Server Foundation is licensed specifically for business use. It doesn't have the client backup found in Windows Home Server, but it can act as an AD domain controller, and you can manage your network clients via Group Policy.

4 **What are the main features in Windows Server Foundation?**—Windows Server Foundation provides networking infrastructure support for functions such as DHCP and DNS. It can supply file and print sharing services. Like a typical Windows server, it can also run line-of-business applications and server products such as Microsoft SQL Server. In addition, it can run Microsoft IIS and provide remote access and Terminal Services.

5 **What are the main limitations in Windows Server Foundation?**—Without a doubt, the most important missing feature is built-in support for virtualization: Windows Server Foundation doesn't include Microsoft Hyper-V. Also, because it's targeted at small businesses, Windows Server Foundation supports a maximum of 15 concurrent users. It runs only on single-socket systems and can access a maximum of 8GB of RAM.

6 **Are there 32-bit and 64-bit versions of Windows Server Foundation?**—Windows Server Foundation is Microsoft's first 64-bit-only version of Windows Server. There is no 32-bit version of Windows Server Foundation.

7 **Is there a Server Core installation option?**—No, Windows Server Foundation doesn't have a Server Core installation mode. However, it does support all the roles and features found in the Windows Server 2008 Standard edition, such as the ability to use the File Services and Print Services roles and the ability to add Windows BitLocker Drive Encryption and Windows PowerShell scripting.

8 **Will there be support for international versions of Windows Server Foundation?**—Microsoft will market Windows Server Foundation in 40 different countries, and it will be available in multiple localized versions. Initially, Windows Server Foundation will be available in English, Chinese, Japanese, Brazilian, Portuguese, Spanish, and Turkish.

9 **How do you buy Windows Server Foundation?**—Windows Server Foundation is not sold as a standalone product. It's available only from OEM hardware vendors—it comes preinstalled on new servers. Manufacturers that offer Windows Server 2008 Foundation server bundles include Dell, HP, and IBM. The starting cost for these bundled systems is expected to be under $1,000.

10 **Can you upgrade from Windows Server Foundation to other editions of Windows Server 2008?**—Yes. Windows Server Foundation can be upgraded to any of the other Windows Server 2008 editions and Microsoft is expected to provide upgrade licensing discounts.

InstantDoc ID 102004

MICHAEL OTEY (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Morales

"Xperf provides valuable information about how applications and systems operate in a production environment."

Examining Xperf

Use this Windows event-tracing tool to improve debugging and system performance

Event Tracing for Windows (ETW) is a fast, built-in Windows tracing mechanism for recording activity events provided by both user-mode applications and kernel device drivers. These events aren't what you'll find in the System or Application event Logs. Rather they're component-specific activity events that let administrators and developers account for specific execution states to help diagnose workload, software, and configuration problems. ETW tracing can be enabled and disabled quickly, and you can enable and disable ETW tracing without having to restart the system or process. Let's look at xperf.exe (Xperf), a tool that's part of ETW, which you can use to learn more about how your system or application works. Before we dig much further, though, we need to review architecture briefly.

ETW and Xperf

ETW comprises four main components:

- Event providers—components that generate activity-specific events. The OS has many built-in event providers.
- Event controllers—programs or utilities that can enable or disable events or groups of events.
- Consumers—can be realtime or post-processing. Post-processing consumers read information from an .etl file.
- Event trace sessions—where buffering and logging occur. Events are buffered and written to an .etl trace file or a realtime event consumer.

The Windows Fundamentals team created Xperf, an ETW controller and consumer that's part of the Windows Performance Toolkit, which you can download at msdn.microsoft.com/en-us/performance/cc752957.aspx. Xperf is built over the ETW infrastructure in Windows and provides some valuable information to help administrators and developers understand how applications and systems operate in a production environment. I'll introduce you to basic usage of Xperf and some common scenarios where Xperf is useful in revealing how your system or application operates under the covers.

Xperf is designed primarily to work on Windows Server 2008 and Windows Vista; however, some of Xperf's functionality will work on Windows Server 2003 and Windows XP. To install Xperf on Windows 2003 or XP, you'll have to first install Xperf on a Vista or Server 2008 system, then manually copy all the files from the installation directory to the Windows 2003 or XP system. For example, if you installed Xperf in a directory called c:\xperf on Vista or Server 2008, you'd simply copy the c:\xperf folder to the Windows 2003 or XP system.

Scenario 1: High CPU-Usage Problem

Say you want to find the process that's hogging a large percentage of your system's CPU. Performance Monitor is a commonly used tool to help determine which process is consuming the CPU when the processor spikes. But you might not be able to correlate the high CPU usage to one process. The Processor\%DPC Time counter in Performance Monitor can help you determine whether the CPU spike is a result of a high level of Deferred Procedure Calls (DPCs)—system interrupts that run in the kernel.

DPCs are issued by kernel drivers, so the challenge in such cases is to identify which driver is responsible for the load on the system from DPC activity. By using Xperf as follows, you can make the driver-identification process much easier.

1. Install Xperf. I suggest installing it in an easy-to-navigate directory, such as c:\xperf.
2. Add the following environment variable (type the variable on one line):

```
NT_SYMBOL_PATH =
  srv*c:\symbols*http://msdl.microsoft.com/download/
  symbols
```

3. From a command prompt, navigate to the Xperf directory and type

```
C:\xperf>xperf -on latency
```

The latency flag tells Xperf to turn on a group of providers to start logging events. These events will be used to help diagnose which driver is consuming the highest percentage of CPU time.

4. Wait for the high DPC activity to occur, by monitoring it with Performance Monitor or Task Manager.
5. Then run this command:

```
c:\xperf -I \kernel.etl -a dpcisr
```

The command tells Xperf to process the default .etl—kernel.etl—and specifies an action (-a). Here the action specified is dpcisr, which will produce a report showing DPC and interrupt service routine (ISR) statistics, as Figure 1, page 12, shows.

In Figure 1, the important area to look at is the Usage column, which

```
DPC Info

CPU Usage Summing By Module For the Whole Trace

CPU Usage from 0 us to 57606961 us:

     CPU 0 Usage
     usec      % Module
       25   0.00 CLASSPNP.SYS
       93   0.00 HTTP.sys
    18013   0.03 NDIS.SYS
     1266   0.00 NETIO.SYS
       44   0.00 Ntfs.sys
      427   0.00 Wdf01000.sys
      662   0.00 afd.sys
    11371   0.02 ataport.SYS
        1   0.00 fltmgr.sys
        7   0.00 hal.dll
       32   0.00 luafv.sys
      305   0.00 netbt.sys
      930   0.00 netvsc60.sys
    17888   0.03 ntkrnlpa.exe
      389   0.00 rassstp.sys
      730   0.00 rdbss.sys
        4   0.00 spsys.sys
       26   0.00 srv.sys
       13   0.00 srvnet.sys
       83   0.00 storflt.sys
    42452   0.07 tcpip.sys
   227623   0.40 vmbus.sys
       34   0.00 watchdog.sys

Total = 14501
```

Figure 1: Xperf displaying the DPC activity per driver

tells you the percentage of CPU activity resulting from DPCs on a per-driver basis. This report provides a convenient means for quickly identifying which driver is responsible for the high amount of CPU usage. What makes this a nice story is that there are no other debuggers to install and no data file that a support professional needs to review. Using Xperf in this way provides an easy method for diagnosing a problem common in production environments.

Xperf is capable of so much more than simply reporting DPC information. Let's look at another usage scenario.

Scenario 2: Uncovering Disk I/O Activity

Have you ever seen your hard drive lights constantly flashing and wondered what files were being accessed and what activity generated so much disk I/O? With Xperf, you can view spikes in disk I/O, then drill down to a specific I/O spike to determine what processes were accessing the disk at that time and what files were being accessed. Here's how to do it:

1. Use the same command as in step 3 in the previous section. If you don't specify a trace file, Xperf uses the default, kernel .etl.
2. Wait for the disk activity to spike.
3. Stop and merge the kernel .etl trace by issuing the command

```
c:\>xperf -d itpro.etl
```

4. Now open the trace in the Xperf viewer by issuing the command

```
c:\>xperf itpro.etl
```

After running this command, you'll see Xperf's Windows Performance Analyzer window, in which you can identify the various spikes in disk I/O activity. However, we need to understand what activity on the system caused these spikes. To do so, simply highlight the spiked activity from within the Windows Performance Analyzer window, right-click it, and select Summary Table. Note that you'll now see a list of processes that generated disk I/O for the time period you highlighted. Click the plus sign next to each process to view the files accessed by these processes and the size of the I/O request, as Figure 2 shows.

From Figure 2, you can clearly see the processes involved in generating the I/O activity and the files accessed. For this example, the MsMpEng.exe process is from the Microsoft Forefront Client Security application, which accessed the edb.log file and the svchost.exe process for Windows Update, then accessed the DataStore.edb and the edb.log file.

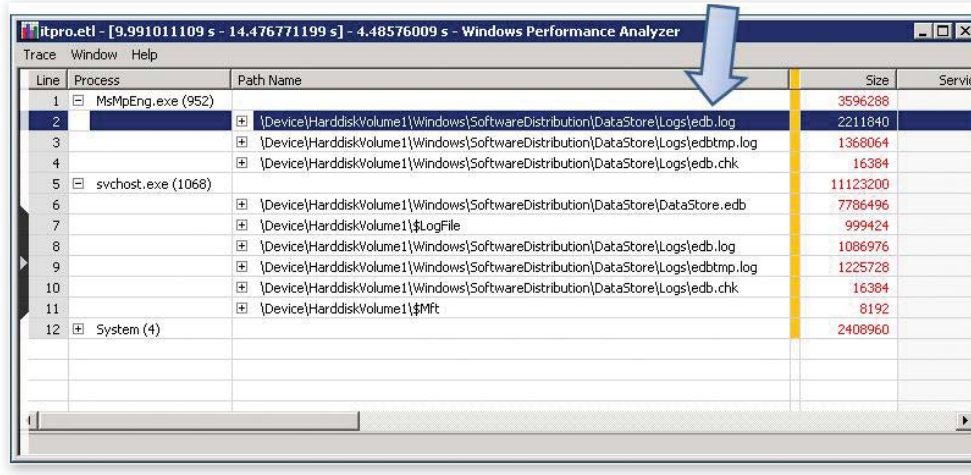


Figure 2: Xperf summary detail view

I did a quick Internet search on edb.log and DataStore.edb and learned that they're files associated with Windows Update. So at the time of my test, Windows Update was running—which requires access to these specific files. And through Xperf, I determined which processes were responsible for generating specific disk activity and what files were accessed during that time. Although this was just a test, you can follow these same steps to determine what processes and files are responsible for generating a high amount of disk activity on your systems.

Power-Packed Utility

There are other utilities that will generate similar information; however, Xperf is a single utility that's capable of much more than what I can cover in one article. In an upcoming article, I'll cover one of the best features of Xperf, the stackwalking profiler, which can help solve process-spike problems by letting you see which modules and functions inside a process are consuming the most CPU.

InstantDoc ID 102054

MICHAEL MORALES (morales@microsoft.com) is a senior escalation engineer for Microsoft's Global Escalation Services team. He specializes in advanced Windows debugging and performance-related issues. For information about Windows debugging, visit blogs.msdn.com/ntdebugging.

Special thanks to Tate Calhoun, a Microsoft escalation engineer who contributed significantly to this article.

TOOL TIME

windowsitpro.com

Build and Burn Image Files with ImgBurn

ImgBurn is cool freeware that lets you work with images files in ISO and many other image file formats (e.g., BIN, IMG, NRG). Although ImgBurn is small (less than 2MB), it offers a lot of functionality. You can use it to build image files and burn them on CD-ROM and DVD disks.

ImgBurn has five modes:

- Read (*Create image file from disc* in the EZ-Mode Picker). You use this mode to read the contents of a CD-ROM or DVD and create an image file on your computer.
- Write (*Write image file to disc* in the EZ-Mode Picker). You use this mode to write image files to a disk. You can queue the image files you want to burn.
- Build. You use this mode to either create an image file from files on your computer (*Create image file from files/folders* in the EZ-Mode Picker) or write the files directly to a disk, without creating an image file (*Write files/folders to disc* in the EZ-Mode Picker).
- Verify (*Verify disc* in the EZ-Mode Picker). You use this mode to determine whether a disk is 100 percent readable and to compare a burned disk's image file against the source image file to ensure the data match.
- Discovery (*Discovery* in the EZ-Mode Picker). You use this mode to check the quality of the burns your drive is producing.

ImgBurn supports all 32-bit and 64-bit Windows OSs (including Windows Server 2008 and Windows 7). After installation, ImgBurn can be copied to a USB drive. You can download ImgBurn from many sites, including its home page at www.imgburn.com. However, people have reported problems with using that site's free download. I had no problems downloading ImgBurn from CNET (download.cnet.com/ImgBurn/3000-2646_4-10847481.html).

—Serge Bedard, technology architect, CSST

InstantDoc ID 102064

- ImgBurn
- Fax Security
- iisweb.vbs
- Strong Passwords
- CPU Loads

READER TO READER

Dumpster Diver Delight

Douglas A. Norris

Be aware that your plain paper fax machine is making two copies of each printed incoming fax. One copy is on paper. The other copy is in the fax film cartridge that you eventually toss into the dumpster. It doesn't take much to recover the images from the discarded roll of film. Although the images will be reversed, you can hold them up to a mirror and easily read them. To avoid this security exposure, you need to destroy the spent film before it reaches the dumpster.

—Douglas A. Norris, IT consultant

InstantDoc ID 102065

Fool iisweb.vbs Into Creating Websites Whose Home Directories Include UNC Paths

The iisweb.vbs script that comes with IIS 6.0 is an incredibly useful tool for creating websites. You run it from the command line with a command such as

```
iisweb /create c:\ana\yeni1 "Site1"
/b 80
```

In this command, C:\ana\yeni1 is the home folder for the website. You can create many websites programmatically using this tool, but it doesn't let you specify a Universal Naming Convention (UNC) path (e.g., \\deryapc\ana\yeni1) for the home directory. So, if you want to create websites whose home folders reside on shares, you can't use this tool.

Fortunately, it's easy to fool iisweb.vbs. I devised a solution that lets you use UNC paths for newly created websites. Let me give an example. Suppose the contents of several websites are located on a computer named Deryapc under a share named Ana. Under Ana there are separate folders for each of the websites. The folders are named yeni, yeni2, and yeni3. Although the websites' contents are on Deryapc, the websites are defined on a computer named Harunpc. Here are the steps to use a UNC path—\\deryapc\ana\yeni1—as the websites' home directory:

1. Create a folder named Ana on Harunpc. This folder serves as a placeholder for the websites.
2. Use iisweb.vbs to create the websites programmatically on Harunpc. In the creation process, specify C:\ana as the new websites' home folders, using the commands

```
iisweb /create c:\ana\yeni1 "Site1"
/b 80
iisweb /create c:\ana\yeni2 "Site1"
/b 80
iisweb /create c:\ana\yeni3 "Site1"
/b 80
```

3. Stop the IIS services.
4. Open the metabase.xml file in Notepad or another text editor. The metabase.xml file, which contains the IIS configuration parameters, resides in the C:\WINDOWS\system32\inetsrv folder.
5. Change the home folder information by specifying \\deryapc\ana as the root folder instead of C:\ana.

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID text box.

Listing 1: ReplaceInMetabase.vbs

```
Const ForReading = 1
Const ForWriting = 2
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile("C:\WINDOWS\system32\inetsrv\metabase.xml", ForReading)
strText = objFile.ReadAll
objFile.Close
strNewText = Replace(strText, "c:\ana\", "\\deryapc\ana\")
Set objFile = objFSO.OpenTextFile("C:\WINDOWS\system32\inetsrv\metabase.xml", ForWriting)
objFile.WriteLine strNewText
objFile.Close
```

(A)

Listing 2: RefreshIIS.bat

```
net stop w3svc
net stop httpfilter
net stop msftpsvc
net stop iisadmin
replaceinmetabase.vbs
net start w3svc
net start httpfilter
net start msftpsvc
net start iisadmin
```

6. Restart the IIS services.

The new websites now point to the shares instead of the local folders.

I use this solution frequently, so I created the ReplaceInMetabase.vbs script in Listing 1 to edit the metabase.xml file. As callout A shows, the script replaces the old string *c:\ana* with the new string *\\deryapc\ana*. To use this script, you simply need to customize the code in callout A with your old and new strings.

I also created another script, RefreshIIS.bat, which Listing 2 shows. This batch file stops the IIS services, runs ReplaceInMetabase.vbs (which edits the metabase.xml file), then restarts the IIS services.

Murat Yildirimoglu

If you want to use the ReplaceInMetabase.vbs script instead of manually editing the metabase.xml file, follow these steps:

1. Create a folder named Ana on Harunpc.
2. Use iisweb.vbs to create the websites programmatically on Harunpc. In the creation process, specify C:\ana as the new websites' home folders.
3. Run RefreshIIS.bat.

You can find the ReplaceInMetabase.vbs and RefreshIIS.bat scripts in the 102053.zip file, which you can download by going to the *Windows IT Pro* website (www.windowsitpro.com), entering 102053 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.

—Murat Yildirimoglu

InstantDoc ID 102053

The Trick to Creating Strong Yet Easy-to-Remember Passwords

One of the biggest security concerns IT departments see in an organization is the protection of passwords. Many times end users aren't aware of the security implications that sharing or not protecting their passwords can have. In most organizations, policies are put in place, but often times the reasons behind those policies are never explained to the end users. It might be very convenient for end users to share a password with another end user when they call in sick or need someone to cover for them. Explaining the security implications of such practices will make sharing passwords much less tempting in those situations.

Another concern with password security is the fact that passwords are only as secure as your end users make them. A strong password security policy is a must, but this, too, is often misunderstood by end users. Passwords quickly become too numerous and lengthy for end users to remember, so the passwords often get written down and hidden somewhere.

To help end users come up with passwords that are strong yet easy to remember, I use this trick: When assisting end users with creating a new password, I suggest that they chose two characters to replace with numbers or symbols. For instance, instead of using the password *Football*, an end user could use the password *F00tb/\ll*. Replacing each occurrence of the letter *o* with a zero (0) and replacing each letter *a* with forward and backward slashes (/\) are easy-to-remember substitutions that help create stronger passwords. The end user can use these substitutions for every password change (e.g., F0rtun/\te), which makes remembering strong passwords much easier and writing passwords down less likely.

Dan Swanson

Believing that end users will blindly follow security guidelines simply because a policy in place is setting yourself up for disaster. An explanation and humanistic approach is often overlooked but can have a significant effect on password compliance in your organization.

—Dan Swanson, client support technician, Mountain Plains Farm Credit Services

InstantDoc ID 102050

A Refreshing Look at CPU Loads

At my company, we occasionally see a rash of slowdowns on our network. In some cases, the slowdowns occur after a patch or a new software package has been deployed. In other cases, there's no apparent reason for the slowdowns. When there's a rash of slowdowns, we run CpuLoadPercentage.vbs to find servers that are running "hot" as we call it. This script helps us find the CPU-hogging servers in a fraction of the time it would take to manually check all of them.

The script returns the value of the CPULoadPercentage property from Windows Management Instrumentation's (WMI's) Win32_Processor class. The CPULoadPercentage property value is an averaged percentage of the load on a particular CPU over a one-second time period. For each server, the script writes the CPULoadPercentage property value to a Microsoft Excel spreadsheet. To make sure a balanced sample is being obtained, the script checks the CPULoadPercentage property value three times in succession. Although the

	A	B	C	D
1	Computer - CPU	Sampling 1	Sampling 2	Sampling 3
2	My-pc CPU0	8	36	27
3				

CPU LoadPercentage

Figure 1: Sample results from CpuLoadPercentage.vbs

Listing 3: Code That Demonstrates How to Use the SWbemRefresher Object

```
strComputer = "."

(A) NumberOfSamples = 5
Set RefresherObject = CreateObject("WbemScripting.SWbemRefresher")
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")

Set ProcessorObjects = _
  RefresherObject.AddEnum(objWMIService,"Win32_Processor").ObjectSet

(B) RefresherObject.Refresh

(C) For i = 1 to NumberOfSamples
  RefresherObject.Refresh
  For Each Sampling in ProcessorObjects
    MsgBox strComputer & "  " & Sampling.DeviceID & "  " & Sampling.LoadPercentage
  Next
Next
```

script is hard-coded to obtain three CPU load readings per server, you can easily modify it to obtain as few or as many readings as you'd like.

Figure 1 shows a simple example of three CPU load percentage readings. If you had multiple servers with multiple CPUs, you'd see a row for each server's CPU.

To get the three CPU load percentage readings, the script uses WMI's SWbemRefresher object, which you can use to obtain and refresh WMI data. Using the SWbemRefresher object's Refresh method is faster and less prone to errors than using the SWbemServices object's ExecQuery method. (For more information about the advantages of using the Refresh method, see the Microsoft article "Don't Panic: You Can Use Scripts to Monitor Performance" at www.microsoft.com/technet/scriptcenter/topics/win2003/perfmon.mspx.)

Creating a SWbemRefresher object is really quite simple. First, you begin by creating an instance of this object, after which you connect to the WMI namespace on the target computer, as callout A in Listing 3 shows. Then, you use the SWbemRefresher object's AddEnum method. To call this method, you need to specify the target computer (in this case, a remote server) and the target class (in this case, Win32_Processor). The ObjectSet property at the end tells the AddEnum method to return a collection of WMI objects.

Next, you call the SWbemRefresher object's Refresh method, which callout B shows. Note that, for some unknown reason, the very first time the Refresh method is called, it won't return any items to the collection. This first instance of the refresh call is referred to as *priming*.

Finally, the code at callout C steps through the collection and reports the CPU load percentage readings. In this code, DeviceID refers to specific CPUs on the server. If you have four CPUs, for instance, you'll see readings for CPU0 through CPU3.

Note that you won't find Listing 3's code in CpuLoadPercentage.vbs. Listing 3 is meant only to show you how use the SWbemRefresher object. To obtain the actual script, you can go to the *Windows IT Pro* website (www.windowsitpro.com), enter 102067 in the InstantDoc ID box, click Go, then click the *Download the Code Here* button.

CpuLoadPercentage.vbs works on Windows Server 2008, Windows Server 2003, Windows Vista, and Windows XP machines. Before you use CpuLoadPercentage.vbs, though, you need to specify the computers for which you want to collect CPU load percentage readings. In the code

```
compArray = array("pc1","Server1", _
  "Server2","trex-pc")
```

replace the dummy names (i.e., pc1, Server1, Server2, and trex-pc) with your computers' names. You can specify any number of machines. Alternatively, you could modify the code to use an organizational unit (OU) or a file to provide the list of computer names.

If you want to change the number of CPU load percentage readings taken, simply change the value of 3 to the desired number in the line

```
NumberOfSamples
= 3
```

Jim Turner

I hope you find this script useful. It helps us spot those servers that need attention a lot faster than checking them all manually.

—Jim Turner, domain administrator and applications developer, Computer Sciences Corporation

InstantDoc ID 102067

"I hope you find this script useful. It helps us find the CPU-hogging servers in a fraction of the time it would take to manually check all of them."

Deep Dive into Windows Server 2008 R2

eLearning series

with John Savill

WHEN
August 20, 2009

WHERE
Your computer

COST
$99

LESSONS
11:00 am EDT
Architecture Modifications and New Features and Capabilities

12:30 pm EDT
Advancements in Hyper-V and Remote Desktop Services

2:00 pm EDT
What's New with Active Directory and Group Policy

HOW
Register at windowsitpro.com/go/elearning/WindowsServer2008R2

Take Your Organization to New Levels!

Join MVP John Savill on August 20, 2009 for 3 informative lessons on Windows Server 2008 R2, plus live Q&A sessions—all on your own computer! Get the skills and tools you need to maximize your Windows Server investment and avoid purchasing third-party software and licenses for capabilities that are provided in-box.

INSTRUCTOR

John Savill is the author of the popular FAQ for Windows and a contributing editor to *Windows IT Pro*. He is an advisory architect for EMC's Microsoft consulting practice, an MCITP: Enterprise Administrator for Windows Server 2008 and a 10-time MVP.

Learn more about the speaker, sessions, and how to reserve your seat at:
windowsitpro.com/go/elearning/WindowsServer2008R2

Windows IT Pro

- Outlook
- Shared Drives
- Solid State Disks
- Windows Server 2008

ANSWERS TO YOUR QUESTIONS

Q: How do I move a Digital ID certificate from one Microsoft Office Outlook installation to another?

A: Moving a certificate isn't difficult if the certificate isn't configured to prevent exporting. Certificates are exported to a file, which can then be imported into another installation of Outlook for the same name and email address.

Digital IDs are managed from the Trust Center in Outlook 2007, found under Tools then Trust Center. Select the E-mail Security option in the left pane. In the middle of the right pane, in the Digital IDs (Certificates) section, click the *Get a Digital ID* button to open your default browser to a Microsoft page listing digital certificate providers for Outlook. Click the Import/Export button to save your digital ID to a file for use in another workstation. For the equivalent in Microsoft Office Outlook 2003, click Tools, Options, and then the Security tab.

The Import/Export button opens the Import/Export Digital ID dialog box. To export the certificate, click the radio button next to *Export your Digital ID to a file* in the lower part of the window. You'll see the Select Certificates box, which lists the certificates available on this installation. You can see the certificate details here by clicking the View Certificate button. This opens the Certificate window. Select the certificate, click OK, and then save the digital ID as a file. Click Browse next to the Filename field and save the certificate in the desired location with either a .pfx or .p12 extension. You can save it to a network share or a USB flash drive if you need to move it to another workstation.

Outlook 2007 has an odd misstep at this point in the process. After naming the certificate file, the interface returns to the import section of the Import/Export Digital ID window. The radio button for the Export part of the interface has to be selected again to add a password for the file, which is mandatory. (Exporting to a file is also a good way to back up your certificates at the client-level.)

To Import the certificate to a new Outlook 2007 installation, you'll follow similar steps. Again, use the Import/Export button in the E-mail Security section of the Trust Center. With the radio button selected next to *Import existing Digital ID from a file*, browse to the certificate file saved during the export, and click OK. You'll also need to enter the password created during the export. Click OK to apply the certificate to this destination installation, ready to use.

If you have a certificate that's centrally managed, or if you have a free certificate provided for personal use on a single workstation, it may be configured to prevent export. Attempts to export a certificate such as this will return an error message stating that *The Digital ID cannot be exported*. This prevents users from exporting their digital IDs, which could then be readily available for misuse.

—William Lefkovics
InstantDoc ID 101948

Q: How can I see which files are open in Windows Server 2008?

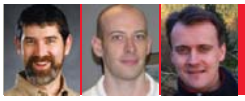
A: The Share and Storage Management Microsoft Management Console snap-in has a handy Manage Open Files action that lets you quickly see which files are open and by whom. Just click this action and you'll get a display of the information you're looking for.

—John Savill
InstantDoc ID 102036

Q: In Windows Vista and Windows Server 2008, when I connect a drive to network share while running in normal user mode, I can't access it from an elevated administrator command prompt window. Is this normal? Is there a way around this?

A: The behavior you experienced is illustrated in Figure 1, page 18. This screen shot shows two command prompt windows. The first is running in the security context of a normal (non-administrator) user, meaning the user has a filtered access token. The second prompt is running in the security context of an administrator account, and the administrator has a full access token. In both windows, the user retrieves a list of currently mapped network drives after mapping a network drive, Z, while running in normal user mode. In the user mode prompt the network drive shows as OK, but in the administrator prompt the network drive shows as unavailable.

This is the default behavior in Vista and Server 2008. Mapped network drives



William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Jan De Clercq | jan.declercq@hp.com

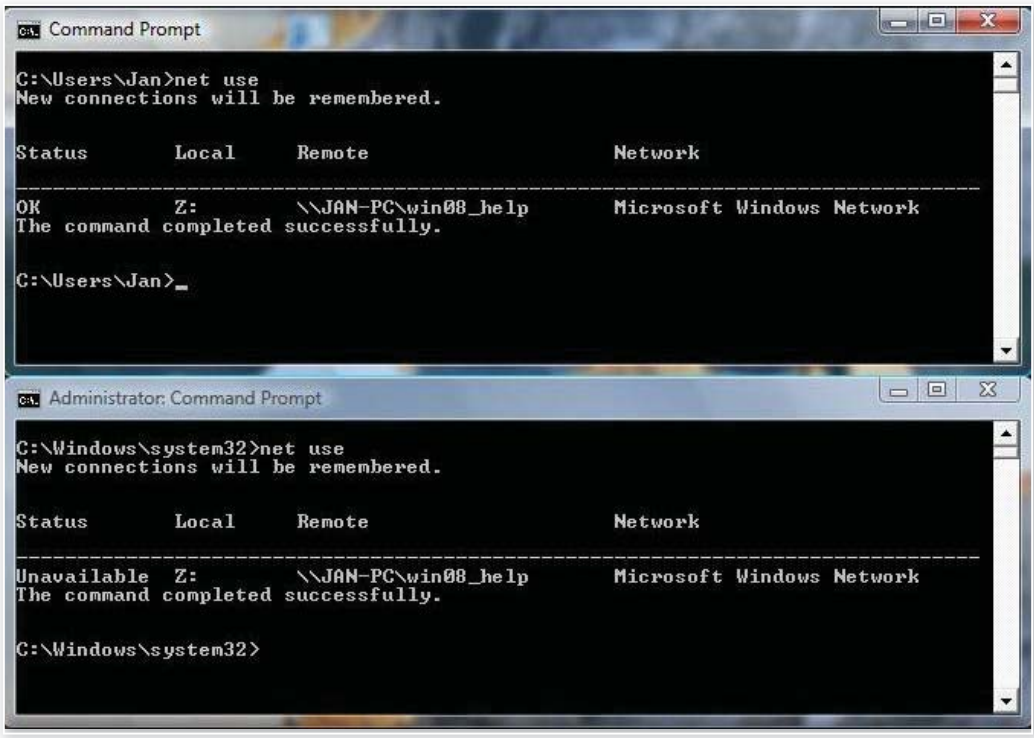


Figure 1: Availability of mapped network drives in normal user and administrator-level command prompt windows

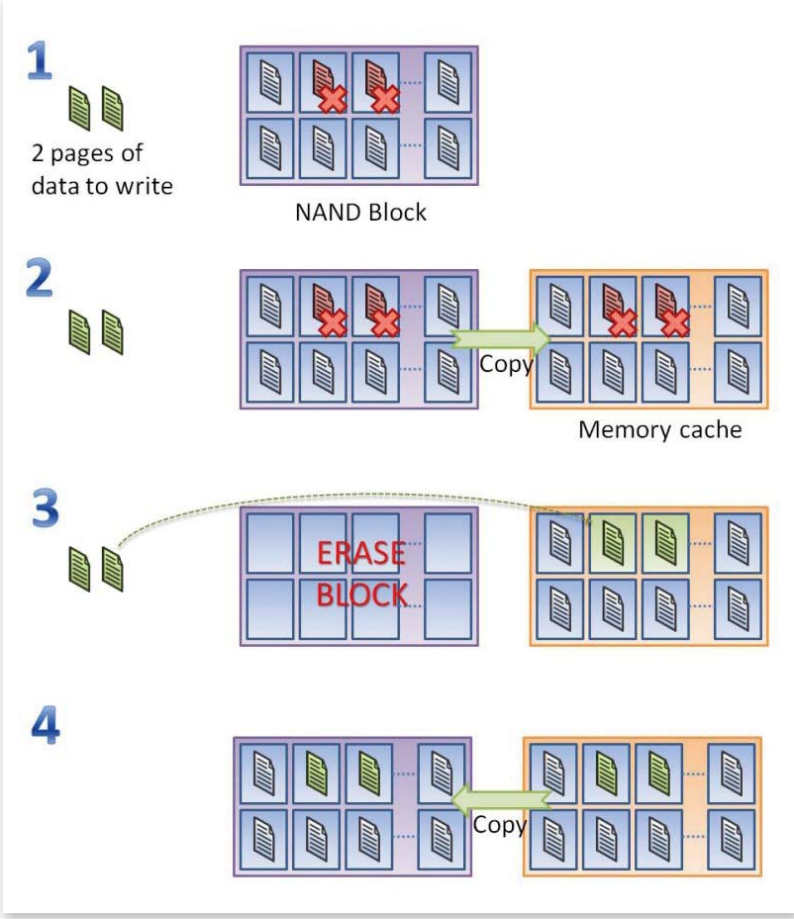


Figure 2: The process for writing to an SSD

become unavailable when switching to another security context. When network shares are mapped, they're linked to the logon session for the current process access token. When you elevate to an administrator command prompt window, a second logon session is created, so the shares mapped in your normal user mode logon session become unavailable.

This default behavior can be changed in the registry. To enable access to mapped network drives from administrator-level security contexts, create a new REG_DWORD registry value named EnableLinkedConnections with a value of 1 in the registry key HKLM \Software\Microsoft\Windows\CurrrentVersion\Policies\System. You must reboot your system for this to take effect.

—Jan De Clercq
InstantDoc ID 102023

Q: I heard solid state disks (SSDs) suffer from a decline in write performance as they're used. Why?

A: SSDs behave very differently from traditional mechanical, platter-based hard disks. SSDs are made up of cells that each store one bit of data (in Single Level Cell, or SLC, drives) or more than one bit (in Multi Level Cell, or MLC, drives, which currently only store two bits per cell but could store more in the future). The two types of SSD are made the same way, but it takes longer to read and much longer to write to MLC, because you have to use larger voltages to check the possible data values.

The cells in an SSD are organized into pages, the smallest unit the SSD can read or write. Pages are normally 4KB. These pages are then organized into blocks, traditionally 128 pages per block, for a block size of 512KB blocks. This is important

because this is the smallest structure that can be erased. You can read and write at a page level, but you can only erase an entire 512KB block—so you can read 4KB at a time and write 4KB at a time to empty space, but you can't overwrite a page.

To overwrite a page, you must first erase its content. Because you can only erase at a block level, you have to read the entire content of a block to memory, replace the pages with new content in memory, erase the entire 512KB block, then write back the entire 512KB block. All of that reading and writing to change even one bit! The good news is that the controller for the SSD has memory and a processor to do this, so you aren't going outside the SSD for the process, which is illustrated in Figure 2.

In step 1, there's 8KB (two pages) of data to write. Two pages on the target block contain deleted data, shown as red pages, and are available to be overwritten. Remember that when you delete a file under NTFS, the data on disk is not actually touched. Rather, the pages are marked as available in the file system.

In step 2, the content of the block is copied to the memory cache. Next, the updated 8KB of data is written in the cache, overwriting the pages that previously contained the deleted data. The block is erased and is completely empty of all 512KB of data. Finally, the updated content of the memory cache is written back to the block.

The firmware in SSDs works around the problem of writing entire blocks to limit overwriting where possible. The SSD will instead write to every page on the SSD before starting to perform overwriting, which requires erase operations. Many SSDs actually ship with additional space they don't advertise so they can delay overwriting.

There comes a point, however, when every page has been written to and you have to start overwriting data. At this point, the SSD has to start using the sequence from Figure 2, which is where you see write operations slow down. Note that read operations aren't affected by this problem.

SSD drives suffer from write degradation over time because more of the writes require erasing whole blocks. There are firmware updates for many SSDs that try to reduce this degradation, but there are limits to what an SSD controller can do. The controller has no idea which data is actually available to be deleted, because the OS never tells it during a delete operation, and the SSD controller only finds out once it gets instructions to overwrite the data.

Remember that the flash memory in SSDs can only be erased a limited number of times before it stops storing data and your SSD is useless, so limit writing to them when possible.

—John Savill

InstantDoc ID 101947

Providing the **vision** and **intelligence** to keep you and your company **competitive** in today's market!

One Place, One Time...

WINDOWS CONNECTIONS

Virtualization CONNECTIONS

MICROSOFT EXCHANGE CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

SQL SERVER CONNECTIONS

SharePoint CONNECTIONS

MICROSOFT ASP.NET CONNECTIONS

VISUAL STUDIO & .NET CONNECTIONS

WinConnections Fall '09

November 9-12, 2009 | Las Vegas, NV

Mandalay Bay Resort and Casino

Celebrate the upcoming release of Exchange Server 2010!!

Exciting Announcements:

Be among the first to get the insiders scoop on the products and technology you rely on!

As a WinConnections attendee, you and your colleague can attend all of the Connections shows, and cross between all of the sessions, at the same time for the same price.

Steve Riley
Senior Security Strategist

Mark Minasi
MR&D
Best-selling Author, Popular Technology Columnist, Commentator

Scott Guthrie
Microsoft
Corporate Vice President, .NET Developer Division

Thomas Rizzo
Microsoft
Director, SharePoint Group

Tony Redmond
HP
Vice President, Innovation and Community, EDS CTO Office, HP

The first 500 paid attendees will be mailed SQL Server 2008 standard with one CAL

CHECK WEB SITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.WinConnections.com • 800.505.1201 • 203.268.3204 • *Register Today!*

Microsoft® TechNet MAGAZINE TECH Conferences Inc. PENTON MEDIA Windows IT Pro

Getting Started with System Center Mobile Device Manager

Take control of your mobile-device fleet in 5 steps

by Paul Robichaux

ILLUSTRATION BY STONEFLYGRAPHICS@GMAIL.COM

As mobile devices get smarter and more robust, their value to users and companies increases—but so does the associated risk. Having on-the-go access to corporate documents, contacts, email, and calendar data can be a productivity boon, but it can also be a major problem if devices with sensitive data are lost or stolen—something that happens all too often.

Microsoft first offered mobile-device synchronization with its Mobile Information Server, the functionality of which was integrated into Exchange Server 2003. Subsequent releases of Exchange have added improved functionality for mobile-device management, but there were still some device-management and security requirements that Exchange alone couldn't meet. In 2008, Microsoft introduced System Center Mobile Device Manager (SCMDM) to provide enterprise functionality for mobile-device management, security, and monitoring. Let's take a look at SCMDM's features, dive into its setup process, and see how it can benefit your environment.

SCMDM Features

SCMDM promises to bring to mobile devices the kinds of management tools and behavior that we're accustomed to on the desktop. To that end, SCMDM offers four primary capabilities: network connectivity, security, device management, and connectivity optimization.

Network connectivity. SCMDM includes a VPN implementation optimized for mobile devices. Mobile devices often disconnect and reconnect without the user's knowledge, potentially changing their IP addresses (and confusing enterprise applications that expect a more stable connection). SCMDM handles network address translation (NAT) so that applications on the intranet don't have to deal with the device's connection behavior.

Security. With SCMDM, mobile devices can be joined to Active Directory (AD) domains, giving you many of the same management capabilities that typical computers have. For example, you can use users' AD credentials to control network access, and you can apply AD Group Policies to mobile devices. SCMDM provides its own remote-wipe implementation, and it includes tools for inventorying devices and checking them for policy compliance.

Device management. Device management in SCMDM involves enrollment. When you enroll a device, you sign it up to receive policy and management settings from SCMDM. Enrolled devices can receive Group Policy settings, and you can use SCMDM to publish

software to devices in a manner similar to the existing AD publishing tools for Windows computers. (You can enroll only devices that are running Windows Mobile 6.1 or later.)

Connectivity optimization. SCMDM acts as a gateway between managed mobile devices and your internal network. As such, SCMDM can cache data (in both directions), aggregate network traffic, and better control how the device and your network talk to each other.

SCMDM and Other Solutions

You might wonder how SCMDM integrates with some of Microsoft's other products. The answer is fairly simple: It can act as a replacement. For example, when you enroll a mobile device in SCMDM, the policies you define in SCMDM replace any policies you've defined for that device in Exchange 2010 or 2007. If you're using System Center Configuration Manager (SCCM) for inventory and software distribution, you'll find that SCMDM replaces its functionality, too. Likewise, the mobile VPN functionality in SCMDM takes the place of VPN connectivity through Internet and Security Acceleration (ISA) Server or Internet Application Gateway (IAG). SCMDM complements these products, replacing their desktop-, laptop-, and server-focused functionality with functionality that's tailored specifically for the constraints of small, mobile, battery-powered devices.

SCMDM Components

SCMDM includes three major server roles that you'll have to install on your network, as you see in Figure 1.

MDM Gateway Server. The MDM Gateway Server lives on your perimeter network. Mobile devices connect to the gateway server through its mobile VPN; the gateway provides a static IP address on the internal network for each device so that internal applications don't have to know when the mobile device's address changes. The gateway is also responsible for pushing Group Policy changes and software updates to the device. The Gateway Server provides a way to connect devices that are never docked with the user's desktop; once a device is connected, the other SCMDM capabilities come into play.

MDM Device Management Server. The MDM Device Management Server is the intermediary between AD and the mobile device. It's responsible for converting Group Policy information into a format usable by the SCMDM client on the mobile device, and it schedules software updates for transmission to enrolled devices. It's also the central point of inventory and reporting data.

MDM Enrollment Server. The MDM Enrollment Server handles the work of enrolling mobile devices for use with SCMDM. In this role, it shares a database of device information with the MDM Device Management Server.

Deploying SCMDM

The process of deploying SCMDM is slightly different from that of Microsoft's other enterprise products. Longstanding products such as Exchange automatically perform many necessary preparation steps, but SCMDM requires both more manual action on your part and a greater degree of knowledge about what the installation operations involve. The basic steps for deploying SCMDM follow.

1. Prepare AD

As you might expect, the first step in an SCMDM deployment is preparing AD to support mobile-device integration. To do this, you must run the ADConfig (adconfig.exe) tool—provided in the ADConfig directory on the SCMDM installation CD—with its /createinstance switch. You must specify the instance name that SCMDM will use. Bear in mind that you can't change the instance name later (although you can change the friendly instance name, which is what users see), so be careful to pick a name that suits your requirements. You might use the name of your company or organization. You'll typically create a single instance in the root domain of the forest. However, every domain that will contain Windows Mobile devices has to either have its own instance or be linked to an existing instance, which you can accomplish with the ADConfig /enableinstance command.

Next, you must create and enable certificate templates, again using ADConfig, this time with the /createTemplates and /enableTemplates switches. These steps ensure that your enterprise certificate authorities (CAs) will have the templates necessary to automatically enroll mobile devices and issue certificates to them.

You must also grant users permission to manage the MDM servers themselves by adding the appropriate accounts to the four groups that the SCMDM installation process creates. The primary group that you'll use for SCMDM administration is the MDM Server Administrators group. There are separate groups for device administrators, device-support technicians, Help desk operators, and users who can see (but not change) SCMDM configurations. The simplest way to manage these groups is to add your SCMDM administrators to the MDM Security Administrators group; members of this group can add or remove members in each of the other MDM groups. Once that's done, the designated security administrators

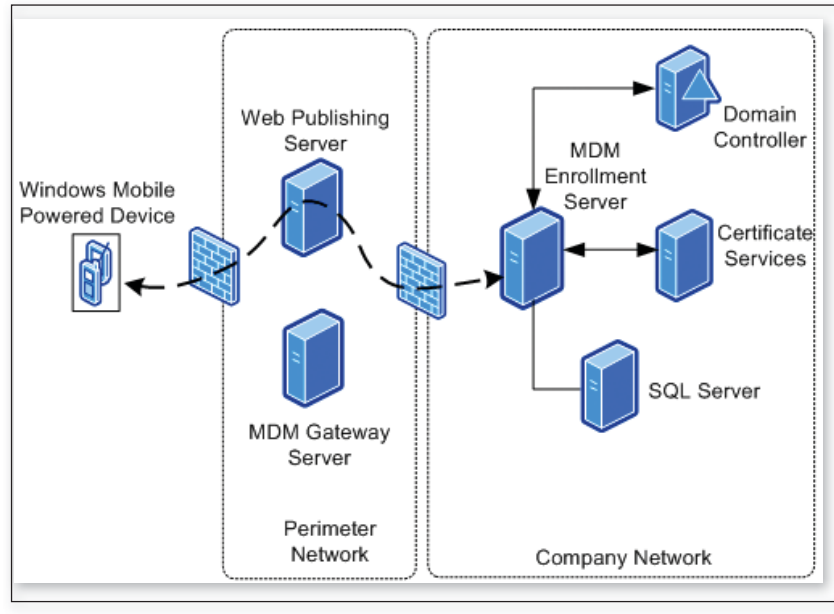


Figure 1: The server roles required for SCMDM

can set up the other group memberships as necessary. The domain's Domain Admins group is automatically added to the MDM Security Administrators and MDM Server Administrators groups.

Because SCMDM will join enrolled mobile devices to the domain, the SCMDM installation creates a new, separate organizational unit (OU)—SCMDM Managed Devices—for mobile devices. You can create additional OUs if you want, or you can just leave this OU alone. However, if you create additional OUs, you'll need to delegate to the SCMDMEnrollmentServers group the permission to create and delete device accounts on the new OUs so that enrollment servers can properly enroll and disenroll devices.

2. Install the Enrollment and Management Servers

Once you've prepared your AD environment, the next step is to install the enrollment and management servers. This is a straightforward process, as long as you've put in place two prerequisite elements: a Microsoft SQL Server 2005 (or later) database instance that the enrollment server and device management server can use to store data about managed devices, and access to a CA that can issue certificates upon request from the enrollment server (for new devices) or for the servers themselves. If you have (or set up) a Windows Certificate Services CA on a server in your organization, the enrollment server can automatically issue certificates to new devices. If not, users might still manually request certificates for their devices, but this detracts somewhat from the inherent value of SCMDM.

You'll also need to specify two fully qualified domain names (FQDNs): one that external users will use to attach to the enrollment server and one for internal connections. These can be the same or different. However, Microsoft's documentation warns that you must enter the FQDN of any load-balancing device that you use, or plan to use, so that issued certificates will have the correct machine names.

3. Install the Administrative Tools

Like Exchange, SCMDM has a suite of administrative tools based on the Microsoft Management Console (MMC) that you can install on any machine in your domain (although you can't use the Group Policy Management Console—GPMC—on 64-bit systems or on Windows Vista SP1). The tools installed include Group Policy Extensions, a management console for SCMDM software distribution, and the SCMDM console itself. You can also manage SCMDM through PowerShell; in fact, many of the configuration tasks you'll need to perform on the gateway server will require you to use the MDM Shell, which is analogous to the Exchange Management Shell.

You'll also want to install the MDM Self Service Portal, an optional component that lets you perform certain device-management activities.

4. Install the Gateway Server

The gateway server is probably the most complicated component of the entire SCMDM package. Think of it as similar in function to ISA Server, which is itself a pretty complicated product to set up. As with ISA Server computers, the MDM Gateway Server isn't usually domain-joined, so you'll have to manually request a certificate for it, then install the certificate (and CA chain) on the machine. You must also export a gateway configuration file, which contains information about the device-management and enrollment servers. During the actual gateway-setup process, you'll provide this file so that the new gateway server can be configured to route traffic to the appropriate device-management and enrollment servers. Finally, you must register the gateway with the other servers by using the Add MDM Gateway wizard in the SCMDM console.

The overall process of installing and configuring the gateway is fairly involved, and I don't have space to fully discuss it here. For a step-by-step guide, see the Microsoft article "Installing MDM Gateway Server" (technet.microsoft.com/en-us/library/dd261827.aspx).

5. Test Your Deployment

Once you've got these components installed, you'll want to try them! The simplest way to do so is to enroll a Windows Mobile device.

Behind the scenes, device enrollment is fairly complicated: The new device must establish an SSL connection to the enrollment server so that it can get the correct set of certificates; then, it establishes a replacement SSL connection using the new certificates so that the enrollment server's identity can be validated. The device then sends a certificate request to the enrollment server, which creates a machine account for the device in AD and forwards the certificate request to the CA. The issued certificate is returned to the device, which installs it, then disconnects from the enrollment server. Neither the administrator nor the device users have to perform these steps manually.

Enrollment is actually a two-step process. First, the administrator must use the MDM management console to create a pre-enrollment request. This step binds an AD user with a particular device, and it also generates an enrollment ID and a one-time password that must be given to the device user. Once the pre-enrollment request is created, the user creates a new connection using the device's Domain Enroll option, entering the enrollment ID and password when prompted. Those credentials provide enough information to jump-start the enrollment process; once it's completed, you can verify that the device has been enrolled by looking for it in the All Managed Devices container in the MDM management console.

Virtual SCMDM

MDM is aimed at enterprise customers who want to bring their mobile devices under the same kinds of management control that they apply to desktop and laptop PCs and servers. Given the increasing capability of mobile devices, for many organizations the benefits of better mobile-device management and control will outweigh the additional cost and complexity of an MDM deployment.

If you want to experiment with MDM, Microsoft has provided the "TechNet Virtual Lab: Using System Center Mobile Device Manager 2008 Features" (go.microsoft.com/?linkid=9637368). When you visit that page and register, a clean lab environment will be automatically built, and you'll have full access to it for 90 minutes. You can also download evaluation versions of the software to test it in your environment.

InstantDoc ID 102071

Paul Robichaux
(probichaux@windowsitpro.com) is a senior contributing editor for *Windows IT Pro*, a founding partner at 3Sharp, and a Microsoft Exchange MVP and MCSE. Paul is the author of *Exchange Server Cookbook* (O'Reilly and Associates) and blogs at www.robichaux.net/blog.

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the newly launched online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.

Featured Product:

Pocket Guide to Group Policy

Learn Group Policy from the inside out with help from *Windows IT Pro* experts such as Darren Mar-Elia and Randy Franklin Smith. Plus find out how to avoid the most common Group Policy mistakes and annoyances found with both Windows 2000 and Windows Vista.

Order your downloadable eBook today for only $15.95*!

left-brain

*Plus shipping and applicable tax.

www.left-brain.com

Windows IT Pro

CONTROL Application Execution with SRP

Use this Group Policy feature to create blacklists or whitelists to control what apps your users run

by Darren Mar-Elia

Users constantly download and run applications they shouldn't, which can result in malware being installed on an organization's network. It's surprisingly difficult to control what users install and execute on their PCs in a Windows desktop world. The first part of solving this problem is making sure that users run their desktops with the least amount of privileges possible—that is, not as administrators or power users unless necessary. The second piece of the puzzle is to control what users can execute.

Many third-party solutions provide application whitelisting or blacklisting—that is, creating lists of applications that are allowed (whitelisted) or not allowed (blacklisted) to run—making it difficult for end users to run code with unknown or unwanted little visitors that can cause problems with your network. However, you can use Group Policy's software restriction policy (SRP, aka Safer) feature to control application execution. Although SRP is missing some features of third-party solutions, such as prebuilt catalogs of application signatures to allow or block, it provides nice capabilities that many IT shops haven't yet discovered or fully exploited.

How SRP Works

SRP is supported on Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP. You'll find it in Group Policy Editor (GPE) under either \Computer Configuration\Windows Settings\Security Settings, as Figure 1, page 26, shows, or \User Configuration\Windows Settings\Security Settings. SRP is available on both the local Group Policy Object (GPO) and domain-based GPOs, but on the local GPO it's available only on a per-computer basis. The power of SRPs comes when you deploy them via domain-based GPOs across multiple systems by using Group Policy's built-in targeting mechanisms.

SRP lets you define application restriction rules within a GPO, and those rules are delivered to the client machine via normal Group Policy processing. Windows stores the rules in the registry and checks them each time a process is executed; if a rule is matched, the application is either allowed or denied, depending on whether it's whitelisted or blacklisted. SRPs don't go into effect on already-running applications, even if Group Policy has applied the rules. It takes a restart of the application for a rule to become effective.

Setting Up SRP

The best way to illustrate how to use SRP is with a typical scenario. For example, I have a business user who runs Microsoft Office and some line-of-business applications. I want to control exactly what that user can execute, so I'm going to implement a whitelist with SRP.

As a best practice, you should create your SRP settings in a separate GPO from other policy settings so that you can disable your restrictions quickly if necessary. You'll need to decide whether to apply your restrictions per-computer or per-user. Per-computer application restrictions apply to anyone who logs on to the computer accounts in Active Directory (AD) that receive those restrictions; this option might be appropriate, for example, when using SRPs against terminal servers. Per-user restrictions are targeted

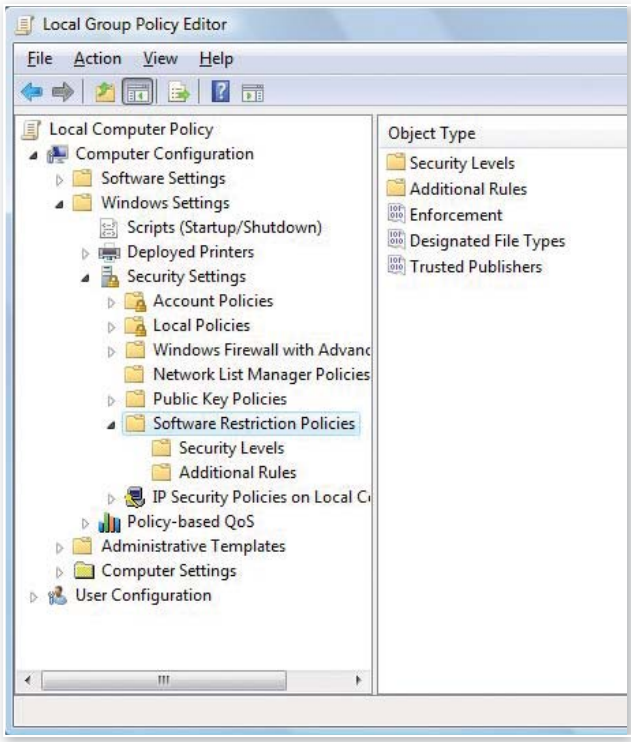


Figure 1: Viewing the Software Restriction Policies node in GPE

toward a given set of user objects in AD and follow those users wherever they log on.

After you decide how to target your policies, the next step is to enable and start configuring your policies. First, start Group Policy Management Console (GPMC) and create your new software restrictions GPO. Right-click the newly created GPO within the Group Policy Objects container in GPMC and choose Edit to bring up GPE, focused on that GPO.

Navigate to the Software Restriction Policies node under Computer Configuration to set per-computer policies or under User Configurations for per-user policies. Right-click the Software Restriction Policies node and choose New Software Restriction Policies. A set of folders and policy items appears in the right-hand pane, which you can see in Figure 1. You might receive a message that a reboot is required before the policies will be enforced (this is true on Server 2008). This message is a bit confusing because you don't need to reboot either the client or server to start receiving these policies.

The first decision with these new items is whether you want to create a whitelist or blacklist. Whitelists create a more secure environment because they deny all code from running except what you explicitly allow. However, whitelists also require more over head to manage, depending on the number of applications in your environment, how often the list changes, and what methods you use to identify them. For our example, we'll create a whitelist.

Double-click the Security Levels folder in the right-hand pane of GPE. On Windows 2003 and XP, the folder contains two nodes: Disallowed and Unrestricted. Server 2008 and Vista add a third node, Basic User. The Unrestricted node (blacklist mode) has a small check mark, indicating that it's the current default. To enable whitelist mode, double-click the Disallowed node and press the *Set as Default* button. Confirm the warning that appears, then close the dialog box to continue.

Basic User is a feature added with the release of Vista. In Basic User mode, users who are administrators on their workstations or AD domains have administrative tokens removed from any applications they run on their system. Essentially, they're prohibited from running any applications with administrative credentials. Behind the scenes, SRP modifies the process token on every application launched by the user to add deny permissions to the following security groups:

- Administrators
- Certificate Admins
- Schema Admins
- Enterprise Admins
- Domain Admins

Think of Basic User as a mechanism for controlling when your administrators are administrators. You might have a set of sensitive computers that contain customer data that administrators occasionally have to log on to. In such cases, you could set Basic User as the default for these computers to prevent users from running applications with their elevated credentials.

Setting SRP Options

Now it's time to set some general options. If you navigate back to the top-level folder within the policy, you'll see three nodes: Enforcement, Designated File Types, and Trusted Publishers. Double-click the Enforcement node to open the Enforcement Properties dialog box that Figure 2 shows. This dialog box lets you control how SRP enforces its rules.

The first option in the dialog box lets you control whether SRP enforces rules against applications or against applications and all of their dependent DLLs. The default, chosen primarily for performance reasons, is to enforce rules against only the calling application. However, if you're concerned about DLLs as possible vectors for attack, you can enable this capability by choosing the All Software Files option.

The lower Enforcement Properties option lets you specify whether SRPs defined in this GPO apply to all users or to all users except members of the local Administrators group. The default is to exclude administrators so that they won't be subjected to the restrictions that have been defined. Keep this as the default unless you really want your administrators to be subjected to the same rules as your regular users.

You define file extensions that SRP considers to be executable types in the Designated File Types node. Initially, you'll see expected file extensions: .exe, .bat, .msi, and so forth. You can add the extensions of other file types you want to control. You don't have to include an extension such as .xls, for example, if you're already creating a rule preventing Microsoft Excel from running.

The third option in the Software Restriction Policies node is Trusted Publishers. This node lets you control aspects of ActiveX controls. You can control whether users can select the publisher of an ActiveX control as a Trusted Publisher. If regular users are free to do so, you end up having no control over which publishers' ActiveX controls are trusted.

Trusted Publishers also lets you control whether Windows checks that certificates

are verified for revocation and valid timestamps before installing an ActiveX control that has been signed by a publisher. Depending on how good your legitimate ActiveX publishers are about keeping their certificates up to date, this might not be a good thing to enable.

Rule Types for Controlling Application Execution

Now let's dive into the heart of leveraging SRP—namely, the rules that control actual application execution. SRP has four rule types to work with:

- hash rules
- path rules
- certificate rules
- network zone rules

You'll probably use hash or path rules for 99 percent of your needs. Certificate rules let you allow or restrict execution depending on whether the code is signed by a particular publisher. Unfortunately, many legitimate applications don't sign their code, so this approach is of limited use.

Network zone rules let you control Windows Installer files—essentially letting you specify which Internet Explorer zone a user can execute .msi files from. Because most malware doesn't ship with a handy Windows Installer file, this feature is at best marginally useful. But if for some reason you need to restrict .msi installations, this rule is your friend.

That leaves us with hash and path rules. Let's look at how each of these works and how you can use them.

Hash Rules

In our whitelisting scenario, all executables are prevented from running unless we specifically allow them. There are a couple of ways to create rules to allow executables. A hash rule is a way of identifying an application by a unique hash that's generated by SRP. Microsoft initially used MD5 as the default hashing algorithm but changed to support the newer SHA-256 in Vista. When you create a hash rule on Server 2008 or Vista, Windows stores both versions of the hash for backward compatibility.

Using hash rules lets you control applications regardless of what users do to circumvent your controls. This means hash rules are probably more useful in blacklist scenarios. Let's say, for example, that you want to prevent a user from running Solitaire (sol.exe) on XP. You'll create the new hash rule in GPE. Right-click the Additional Rules node in the right-hand pane and choose New Hash Rule. In the New Hash Rule dialog box, click Browse and browse to C:\Windows\System32\sol.exe, then click OK. As Figure 3 shows, you can now set the security level to Disallowed to prevent users from running the application.

Figure 2: Viewing Enforcement options for SRPs

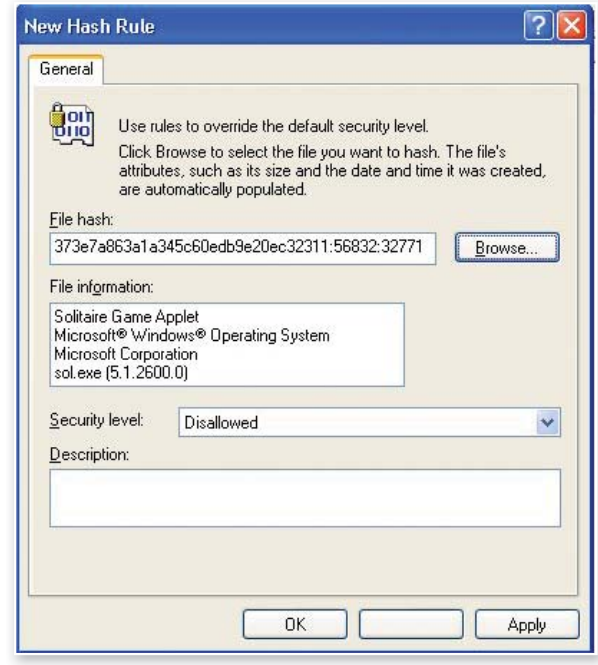


Figure 3: Creating a hash rule for Solitaire

Even if users move sol.exe or rename the executable, the hash rule ensures that the restriction you put in place is maintained. Hash rules are useful for applications that don't change often; however, when the application changes due to an update or patch, its hash value changes and you have to re-do your hash rule. Note that when you specify the executable to control, you should use the version of the application that is specific to your target machines. For example, if you want to restrict Solitaire on XP SP3, you should browse to the version of the executable running on an XP SP3 machine to let SRP calculate the hash.

Path Rules

Path rules are the most useful and powerful of the four SRP rule types. As the name implies, you can specify a path to allow or disallow (or set to Basic User) for execution, and all applications within that path are put under the control of SRP. Creating a path rule is as simple as right-clicking the Additional Rules folder within GPE and choosing New Path Rule, then entering the path on which you wish to create a rule.

The power in path rules is that they can take many forms. For example, a path rule could be something as simple as

```
Sol.exe or Sol.* or S*.*
```

which would prevent users from executing sol.exe, and executables named Sol with any file extension, and any program within

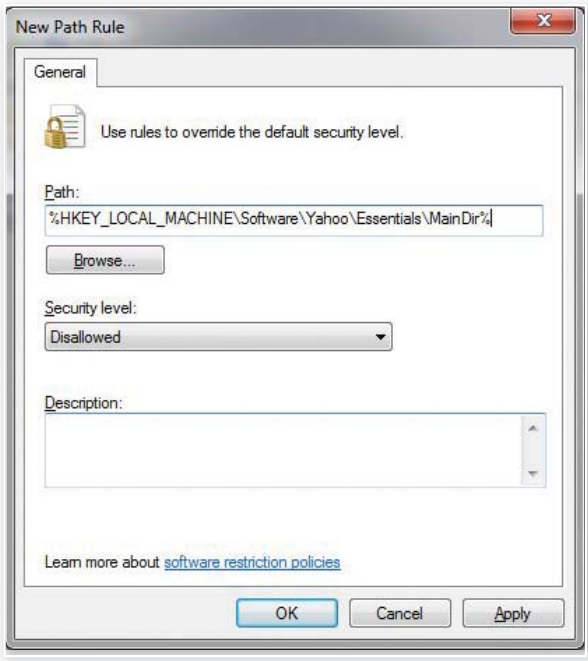


Figure 4: Creating a registry path rule to disallow Yahoo! Messenger

the Designated File Types that starts with *s*. Of course, a path rule can contain an actual path, such as C:\Program Files\Microsoft Office. In this example, all applications within the Microsoft Office folder, including child folders, would be subject to the rule. You can also use UNC paths within path rules. So you could say that only apps found in \\MyServer\Apps are allowed to run. Note that a path rule of \\MyServer\Apps gets resolved to any representation of that same path (e.g., \\10.5.1.1\Apps or P: where P is mapped to \\MyServer\Apps).

Finally, and perhaps most powerfully, you can create registry path rules. You don't always know where a particular application is installed. For instance, by default Yahoo! Messenger installs under C:\Program Files\Yahoo!\Messenger, but a user could choose a different location to install it. How do you create a rule that covers any place an application might be installed? That's where registry path rules come into play.

A registry path rule is a reference to a location in the registry that points to a file system path. In our example, when Messenger is installed, it creates a registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Yahoo\Essentials called MainDir, which contains the path to where Messenger is installed. You would create a registry path rule to prevent Yahoo! Messenger from running the same way you create other path rules; Figure 4 shows what it would look like.

Note that the registry path is entered all the way to the value that contains the file path you want to restrict and must be surrounded by the percent (%) character. In the registry, that value shows up as C:\Program Files\Yahoo! When the path rule is evaluated, SRP looks in the registry to find the path to Messenger, and controls all applications under that path.

Another great use for registry path rules is for preventing execution of code that a user has downloaded as an attachment or from a web browser. For example, let's say you want to prevent users from running apps within Internet Explorer without first saving the file. When a user clicks Open on the download dialog box, IE uses the path to the temporary download location within the registry under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Directory. If you create a registry path rule to this location and set it to Disallowed, no application type that's in your Designated File Types list can execute from that Open prompt.

Microsoft's Pre-Created Path Rules

When you first create a new SRP within a GPO, you'll notice that Windows automatically creates registry path rules under the Additional Rules node within GPE. These pre-created registry path rules set all applications within C:\Windows and C:\Program Files (or on whatever path these well-known folders exist) to be unrestricted. I think Microsoft did this to ensure that when you first set up an SRP whitelist, you don't shoot yourself in the foot and prevent key OS components from running correctly.

However, you do need to be aware of these pre-built rules because if you're trying to create a true whitelist, you might not want to allow all programs within C:\Windows and C:\Program Files to execute. Make sure you test thoroughly if you decide to remove these predefined rules. In fact, if you do want to modify them, I recommend removing only the Program Files rule and leaving the C:\Windows rule in place to ensure no applications that are key to the OS's proper functioning are prevented from running.

SRP Interaction

If you define SRPs across multiple GPOs, you need to know how they interact. For general options such as whether you're in whitelist or blacklist mode, what file types are in use, trusted publisher settings, and so forth, the effective setting is the one that's processed last when Group Policy processing runs on the client. However, rules are essentially merged. This situation can get tricky because you might have a path rule and a hash rule that contradict each other. In this case, the most specific rule wins.

For example, if you have a hash rule that prevents C:\Windows\regedit.exe from running and a path rule that allows everything in C:\Windows to run, the hash rule wins because it's more specific—it points to a specific file. Thus, regedit.exe won't run even though everything else in C:\Windows will. The bottom line is you should try to avoid having overlapping rules across multiple GPOs.

Give SRP a Spin

SRP provides a powerful mechanism to control application execution on Windows systems without costly third-party solutions. It requires a bit of work, and it's not foolproof, but you can get creative with path rules and even hash and certificate rules to create an environment where your users have access to and can execute primarily code that you know is good. I encourage everyone out there struggling to rein in their users' habits of downloading and running untested code to give SRP a spin and see if they can make their environment safer.

InstantDoc ID 102123

Darren Mar-Elia
(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and founder of SDM Software (www.sdmsoftware.com). He maintains a Group Policy resource website (www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).

5 WAYS TO MANAGE SERVER CORE

Get reacquainted with the command line

by J. Peter Bruzzese

If you've taken the time to install Server Core—Windows Server 2008's alternative OS, with its lighter footprint and smaller attack surface—you've been struck by the return of the much loved/hated command line. I don't mean PowerShell (available in Server 2008 R2), but the old cmd.exe. As you dust off your DOS guides and refresh your memory about how to use the command line, you'll need to attend to several other important tasks as well.

First, you need to configure your Server Core system: Join the domain, and possibly change computer names, IP address configuration, firewall settings, Windows Update settings, and so on. Second, you need to enable the roles and features that you want to run under Server Core. Note that Server Core doesn't include Server Manager, so you'll have to use the OCList and OCSetup command-line tools. (For more information about configuring Server Core, see Top 10, "Essential Server Core Setup Commands," InstantDoc ID 98777.) Finally, you need to manage your Server Core system.

The five Server Core management techniques I present here include one local method and four remote methods. Only one of the methods uses a GUI console—so get ready to re-embrace the command line.

1. Local Command Prompt

The easiest way to manage Server Core is to use the local command prompt (i.e., cmd.exe). If you prefer to use a GUI tool to configure Server Core, you can download the Server Core Configurator from www.codeplex.com/CoreConfig. You can use several GUI tools within Server Core as well, such as Notepad, Taskmgr (for Task Manager), Regedit (for the Registry Editor), timedate.cpl (for the Date and Time applet) and intl.cpl (for the Regional and Language Options applet).

For more information about configuring Server Core, including configuration commands, see Microsoft's "Server Core Installation Option of Windows Server 2008 Step-By-Step Guide," at technet.microsoft.com/en-us/library/cc753802.aspx. For information about specific commands, see the Microsoft TechNet A-Z command-line reference page, at technet.microsoft.com/en-us/library/cc778084.aspx. Finally, for videocasts about managing Server Core through Terminal Services, RemoteApp, Windows Remote Shell, and MMC snap-ins, see the bulleted list at the end of the web version of this article (www.windowsitpro.com, InstantDoc ID 101740).

2. Terminal Services

If you use Terminal Services to manage Server Core, you're actually connecting remotely for administrative purposes, so you must edit the registry to enable the Remote Desktop for Administration feature. To enable Remote Desktop for Administration on a Server Core system, go to the command prompt and enter

```
Cscript c:\windows\system32\scregedit
  .wsf /ar 0
```

You should receive output indicating that the registry has been updated.

If the Server Core system has a firewall enabled, you need to open the RDP port to allow the connection. To open the RDP port, enter

```
netsh firewall add portopening TCP
  3389 RDP
```

Once your Server Core system is set up, open the RDP connection from another system. A quick way to accomplish this is to enter

```
mstsc.exe
```

in the Start menu's instant search bar. Then, enter the IP address (or the server name if DNS is configured) and provide the logon credentials. The remote desktop screen will open as a command prompt, with the blue desktop background.

The benefit of this type of connection over a RemoteApp connection (which I discuss in the following section) is that you can still run other applications outside of the command line on your remote desktop. When your work is complete, you can just enter

```
logoff
```

to close the connection.

3. Terminal Services with RemoteApp

Using an RDP connection to connect to the entire system might seem like overkill—especially if you only need the command prompt. Alternatively, you can use a new Server 2008 Terminal Services feature called RemoteApp. This feature lets you create an RDP connection that opens only the command prompt rather than the entire desktop. Before you begin, follow my previous instructions to enable Terminal Services connections.

To create a RemoteApp .rdp file, you need to install the Terminal Services role on a non–Server Core Server 2008 server. You can use Server Manager to accomplish this task.

After you install the Terminal Services role, select the TS RemoteApp Manager option from the Start menu, under Administrative Tools, Terminal Services. The RemoteApp Manager console will open.

Next, select the option to connect to another system, and choose the Server Core system. In the Actions pane on the far right, select Add RemoteApp Programs and locate the cmd.exe application (typically located under c$\windows\system32\cmd.exe). From the Allow list, select Remote cmd.exe. Then, select *Create RDP package* in the Actions pane.

After the package is created, you can double-click to open only the command prompt in a Terminal Services session. In addition, you can send the cmd.rdp file to other users who need to access the Server Core system in a RemoteApp command line.

4. Windows Remote Shell

Windows Remote Management (WinRM) is an implementation of the WS-Management protocol (a SOAP-based firewall-friendly protocol) that allows interoperability between the OS and a variety of hardware vendors. In addition, WinRM lets you connect to a Server Core system and work within a command prompt without creating a Terminal Services connection. One of the benefits of using WinRM is that it uses HTTP port 80 (or HTTPS port 443) to establish the connection. Because these ports are typically already open on firewalls, establishing the connection is quite easy. The idea is that you create a system that is a WinRM listener on one side (the Server Core machine), then use the WinRS tool to connect to that machine.

Before you begin, you need to join the Server Core system to the domain and log on to the domain at least once as an administrator on the Server Core machine. (Note that you must use a Windows 7, Server 2008, Windows Vista, or Windows Server 2003 R2 system to make the connection.)

Go to a command prompt on the Server Core system you want to administer and enter

```
WinRM quickconfig
```

Then, on the system you want to administer the Server Core machine from, enter the command you want to run, as follows:

```
winrs -r:<ServerCoreSystemName>
  <command>
```

You can initiate any command (e.g., dir, ipconfig), but an ideal approach is to issue the cmd.exe command, which fully connects your command prompt to the Server Core machine. Then, any command you enter will run on the Server Core system, and you don't have to reenter the entire winrs command.

5. MMC Snap-Ins

The Microsoft Management Console (MMC) provides a GUI method of administering

Table 1: Rule Group Names for MMC Snap-Ins

MMC Snap-In	Rule Group Name
Event Viewer	Remote Event Log Management
Services	Remote Services Management
Shared Folders	File and Printer Sharing
Task Scheduler	Remote Scheduled Tasks Management
Reliability and Performance Monitor	Performance Logs and Alerts (and File Printer and Sharing)
Disk Management	Remote Volume Management
Windows Firewall with Advanced Security	Windows Firewall Remote Management

Server Core. But before you can run the standard consoles, you must do some command-line work. First, you need to configure the firewall on your Server Core system to allow MMC snap-ins to connect.

Go to a command prompt and enter

```
netsh advfirewall firewall set rule
  group="remote administration" new
  enable=yes
```

To allow only specific snap-ins, enter

```
netsh advfirewall firewall set rule
  group="<rulegroup>" new enable=yes
```

I prefer to allow all snap-ins to connect. If you'd rather enable only the snap-ins you need, you must know the rule group names that correspond to the snap-ins. Table 1 provides this information. In order to use MMC snap-ins to manage a Server Core system, you must have administrative privileges on the system.

You need to consider whether the Server Core system you want to manage is a domain member. If the system is part of the domain, simply open the MMC console, right-click the hierarchy to select *Connect to another computer,* and enter the name of the Server Core system.

If the Server Core system you want to manage doesn't belong to the domain, you must use administrative credentials to create a connection to the Server Core system from your client machine. To do so, open a command prompt on the client machine and enter

```
cmdkey /add:<Server Core System Name>
  /user:<Administrator Account User
  Name> /pass:<Administrator Password>
```

You can then manage the Server Core machine as you would any other system in the domain.

Multiple Management Options

Now that you have more than one point of entry, you can use your command-line skills to take full advantage of Server Core. Server 2008 R2 will include the ability to run PowerShell also, which will undoubtedly increase your ability to administer Server Core both locally and remotely.

InstantDoc ID 101740

J. Peter Bruzzese
(jpb@cliptraining.com), Triple-MCSE, MCT, MCITP: Messaging, is a *Windows IT Pro* contributor and author of *Server 2008 How-To* (Sams). He is cofounder of ClipTraining.com.

PS>dir

Emulating the Dir Command in PowerShell

Try this handy Windows PowerShell script that mimics the way dir works in Cmd.exe

by Bill Stewart

Using Windows PowerShell is a paradigm-shifting experience for Windows users who are accustomed to the Cmd.exe command shell. PowerShell is much more powerful and flexible, but most Cmd.exe commands don't have direct PowerShell equivalents. For example, PowerShell has a default dir alias that runs the Get-ChildItem cmdlet, but Get-ChildItem doesn't behave exactly the same as Cmd.exe's dir command.

Because dir is probably the command I use most frequently in Cmd.exe, I found myself missing some of dir's features when working in PowerShell—in particular, its /a (select attributes) and /o (sort order) parameters. Table 1 shows some example Cmd.exe dir commands and their PowerShell equivalents. As you can see, the PowerShell commands are all longer—and in many cases more complex—than the equivalent dir commands in Cmd.exe. To improve my productivity at the PowerShell command line, I wrote a script, D.ps1, which emulates a number of dir's most useful features.

Introducing D.ps1

You can download D.ps1 by going to www.windowsitpro.com, entering 101900 in the InstantDoc ID box, then clicking the *Download the Code Here* button. Table 2 describes D.ps1's command-line parameters. The main difference between using D.ps1 and using dir in Cmd.exe is that you use a dash (-) instead of a forward slash (/) for the parameters. All of the script's parameters are optional. If you run the script without parameters, it lists the contents of the current directory.

D.ps1 counts the number of files and directories, totals the lengths of the files, and reports them at the end of its output, as dir does. Figure 1, page 34, shows an example of D.ps1's output that displays the JScript script files in the current directory, sorted by date. Note that D.ps1's output doesn't include the displayed directory's path as Get-ChildItem and the dir command do. D.ps1 also displays each file's attributes, which Get-ChildItem does but dir doesn't do. Table 3, page 34, shows some sample D.ps1 commands and a description of each command.

By default, D.ps1 outputs formatted strings rather than file system objects. If you want to output objects or you want to list items from a location other than the file system, you must specify the -defaultoutput parameter, as noted in Table 2. If the current path isn't in the file system (e.g., HKCU:\) and you don't specify a path to list, D.ps1 outputs an error unless you use -defaultoutput.

The script is composed of a param statement, which defines the script's command-line parameters, and six functions: usage, iif, get-attributeflags, get-orderlist, get-providername, and main. The last line of the script executes the main function, which calls the other functions as needed.

The usage and iif Functions

If the -help parameter is present on the command line, the main function executes the usage function. The usage function simply outputs a usage message and ends the script with the exit statement.

The iif function provides a shortcut for the following frequently used syntax:

```
if (condition) {
  $variable = truevalue
} else {
  $variable = falsevalue
}
```

By using the iif function, you can write this instead:

```
$variable = iif { condition }
  { truevalue } { falsevalue }
```

The iif function uses three script blocks as parameters. It executes the first script block; if the result is true, the script executes the second script block—otherwise, it executes the third script block.

The get-attributeflags Function

The main function uses the get-attributeflags function to convert the -attributes parameter's argument (a string containing a list of file attributes to include or exclude) into two bitmap values. If you aren't familiar with bitmap values, see the web-exclusive sidebar "Understanding Bitmap Values," www.windowsitpro.com, InstantDoc ID 101898.

The get-attributeflags function first creates a hash table that contains the attribute characters and their associated .NET bit mask values. It then builds a string based on the hash table's keys, iterates each character in the attribute string, and uses the switch statement to decide whether to enable or disable bits in the returned values. If the attribute character isn't a dash or a valid attribute character, the function throws an error, ending the script. The last line of the get-attributeflags function returns the two bitmap values to the main function; these values are used later in the script.

The get-orderlist Function

The main function uses the get-orderlist function to output a list of hash tables that determines the sort order for the directory listing. The main function passes three parameters to the get-orderlist function: the -order parameter's argument (a string

Table 1: Cmd.exe Dir Commands and Their PowerShell Equivalents

Action	Cmd.exe	PowerShell
List files sorted by date	dir /o:d	gci | sort LastWriteTime
List file owners	dir /q	gci | get-acl | select Path,Owner
List files without the archive attribute*	dir /a:-a	gci | ? {($_.Attributes -band [System.IO.FileAttributes]::Archive) -eq 0}

* The ? character in the PowerShell command is an alias for the Where-Object cmdlet.

Table 2: D.ps1's Command-Line Parameters

Parameter	Description
-path:*path*	Specifies the paths to list. Wildcards and multiple names separated by commas (,) are permitted. You can omit the parameter name (-path) if you use the parameter names for all of the other parameters or if the *path* argument is first on the script's command line. Unless you use -defaultoutput, the paths must be in the file system.
-attributes:*list*	Displays items matching the named attributes. The allowed attributes are: A (ready for archiving), D (directories), H (hidden), I (not content-indexed), L (links), N (no attributes), R (read-only), and S (system). To exclude an attribute, prefix it with '-' (e.g., -D). Use an empty string to include all attributes (e.g., ''). Multiple attributes are permitted.
-order:*list*	Displays items in the specified order. Specify D to sort by date, E to sort by extension, G to group directories, N to sort by name, and S to sort by size. Use '-' before a letter to sort in descending order (e.g., -N). Sorting is performed in the order you specify; for example, -order:E-N sorts the overall list by extension in ascending order, then by name in descending order within each extension grouping.
-timefield:*field*	Controls which time field is displayed or used in sorting. You can specify A (last access time), C (creation time), or W (last write time). W is the default.
-fullname	Displays items' full names.
-recurse	Recurses through subdirectories (equivalent to dir /s). When using -recurse, note that the -path parameter must contain only directory names.
-bare	Displays items' names only.
-q	Displays the owner for each item.
-literalpath	Specifies that paths are literal; that is, no characters in paths are interpreted as wildcards.
-defaultoutput	Outputs objects instead of formatted strings.
-help	Displays a usage message.

Note: All parameters are optional, and all parameter names can be shortened to their first character (e.g., -a:DH is equivalent to -attributes:DH, -r is equivalent to -recurse).

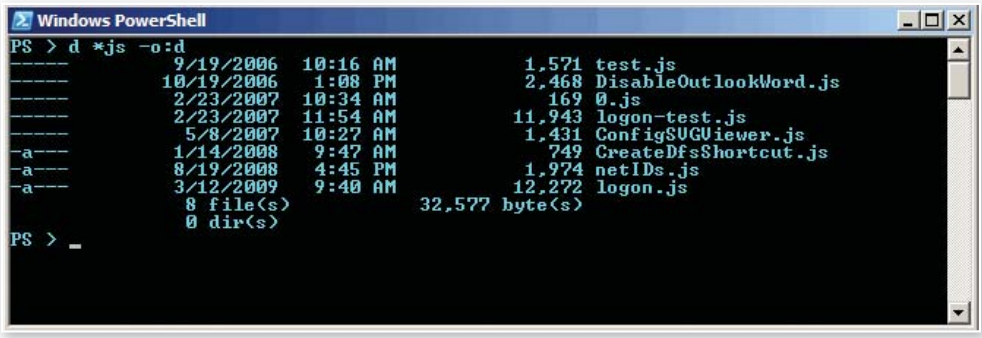


Figure 1: Sample output from D.ps1

Table 3: Sample D.ps1 Commands

Command	Description
d $ENV:SystemRoot	Lists the contents of the OS installation directory.
d c:\ -a:h -recurse	Lists all hidden files and directories on drive C.
d d:\ -a:-dh -recurse	Lists all hidden files on drive D; directories are excluded.
d \\server1\Users\ spacehog -o:-s -recurse	Lists the contents of the spacehog directory sorted by file size (largest files first).
d c:\data*.xl* -o:d	Lists *.xl* files in C:\data sorted by LastWriteTime (oldest files first).

containing the desired sort order), the name field (the property to use when sorting by name), and the time field (the property to use when sorting by date). Each hash table has two keys: Expression and Ascending. The Expression key in each hash table is the sort expression, and the Ascending key can contain either $TRUE (for an ascending sort) or $FALSE (for a descending sort).

The get-orderlist function works similarly to the get-attributeflags function: It creates a hash table containing the sort-order characters, builds a string based on the hash table's keys, iterates each character in the sort-order string, and uses the switch statement to output a hash table for each valid character. If the sort-order character isn't valid, the function throws an error. The main function uses the hash table (or tables, if it returns more than one) returned from the get-orderlist function with the Sort-Object cmdlet later in the script.

The get-providername Function

The get-providernamefunction, which Listing 1 shows, determines a path's provider (e.g., FileSystem, Registry, Certificate). The function returns an empty string if the path doesn't exist. First, the function sets the $result variable to an empty string; then, using the iif function, it sets the $pathArg variable to either -literalpath or -path according to the state of the script's -literalpath parameter. Then the function sets the $ErrorActionPreference variable to SilentlyContinue to prevent PowerShell from displaying error messages in case an error occurs.

Next, the function uses the Test-Path cmdlet to check whether the path exists. However, it uses Invoke-Expression rather than executing Test-Path directly so that it can support the script's -literalpath parameter. The function uses the backtick (`) escape character before the $path variable to prevent PowerShell from expanding the variable. If the path exists, the script uses the Invoke-Expression cmdlet—again, to support -literalpath—to execute the Get-Item cmdlet and select the first returned object. The function then assigns the object's PSProvider object's Name property to the $result variable. The last line of the function outputs the $result variable.

The main Function

The main function contains the main body of the script. First, if the -help parameter is present, the main function calls the usage function, which would display the usage message and end the script. If -help isn't present, the function checks for the -path parameter. If it's missing, the function assumes the user wants to list the items in the current location.

Next, the main function uses the iif function to set the $pathArg variable to -path or -literalpath, depending on whether the script's -literalpath parameter is present or missing. After this, the function checks to see if the -attributes parameter is present. If it is, the main function calls the get-attributeflags function to retrieve the two bitmap values corresponding to the -attributes argument's parameter.

If the -timefield parameter is present, the main function then uses the switch statement to see if the parameter's argument (i.e., the $TimeField variable) starts with *a*, *c*, or *w*, which corresponds to LastAccess-Time, CreationTime, or LastWriteTime, respectively. If the -timefield parameter's argument doesn't start with *a*, *c*, or *w*, the main function throws an error, ending the script. If the -timefield parameter is missing, the main function sets the $TimeField variable to LastWriteTime. The function uses the $TimeField variable to determine which file property to display or use when sorting.

If the -fullname or -recurse parameters are present, the main function uses the iif function to set the $nameField variable to FullName; otherwise it sets it to Name. The function uses the $nameField variable to decide which property to use when displaying or sorting files.

At this point, the main function has processed the script's command-line parameters and is ready to execute the Get-ChildItem cmdlet. However, the script can only implement the -attributes and -order parameters by piping Get-ChildItem's output to other cmdlets. The main function accomplishes this by building a string containing a pipeline. As the code in Listing 2 shows, the main function constructs the pipeline string as follows:

1. If the -recurse parameter is present, the function appends the -recurse parameter to the pipeline.
2. If the -attributes parameter is pres-

Learning Path

WINDOWS IT PRO RESOURCES

Check out these articles for related PowerShell concepts:

"Q. How can I launch a Windows PowerShell instance to run a command from a cmd.exe prompt?" InstantDoc ID 101752

"PowerShell 101, Lesson 3: How to use PowerShell's operators and wildcards," InstantDoc ID 98177

"PowerShell 101, Lesson 4: How to properly use quotes when working with strings," InstantDoc ID 98447

"Iterating Through Collections with PowerShell's foreach Loops," InstantDoc ID 99873

"Test for Numerous Conditions with PowerShell's switch Statement," InstantDoc ID 100411

Listing 1: Get-providername

```
function get-providername($path) {
  $result = ""
  $pathArg = iif { $LiteralPath } { "-literalpath" } { "-path" }
  $ErrorActionPreference = "SilentlyContinue"
  if (invoke-expression "test-path $pathArg `$path") {
    $result = (invoke-expression ("get-item $pathArg `$path -force |" +
      " select-object -f 1")).PSProvider.Name
  }
  $result
}
```

Listing 2: Creating the Pipeline String

```
$pipeline = ""

if ($Recurse) {
  $pipeline += " -recurse"
}

if ($Attributes -ne $NULL) {
  $pipeline += " -force"
  if (($attrInclude -ne 0) -or ($attrExclude -ne 0)) {
    $pipeline += " | where-object { "
    if (($attrInclude -ne 0) -and ($attrExclude -ne 0)) {
      $pipeline += "((`$_.Attributes -band $attrInclude) -eq $attrInclude) -and " +
                   "((`$_.Attributes -band $attrExclude) -eq 0)"
    } elseif ($attrInclude -ne 0) {
      $pipeline += "(`$_.Attributes -band $attrInclude) -eq $attrInclude"
    } else {
      $pipeline += "(`$_.Attributes -band $attrExclude) -eq 0"
    }
  $pipeline += " }"
  }
}

if ($Order -ne $NULL) {
  $pipeline += " | sort-object `$Order"
}
```

ent, the function appends the -force parameter to the pipeline.

3. If either of the attribute bitmap values are non-zero, the main function appends a Where-Object script block to the pipeline; the Where-Object script block isn't necessary if the user wants to see all files, regardless of attributes. The Where-Object script block uses the comparison techniques described in the "Understanding Bitmap Values" web-exclusive sidebar to create a filter that includes or excludes file attributes based on the two bitmap values returned from the get-attributeflags function.

4. If the -order parameter is present, the main function appends the Sort-Object cmdlet to the pipeline.

Next, the main function checks whether the -defaultoutput parameter is present. If it is, the function executes Get-ChildItem by using the Invoke-Expression cmdlet, and then it uses the return statement to return from the main function, ending the script.

If the -defaultoutput parameter isn't present, the main function creates a string containing a formatted string expression that uses the -f operator. Later, the function uses the Invoke-Expression cmdlet to output this string for each file system item it displays. The formatted string expression contains the fields in the expression, the -f operator, and the following properties for each item:

- Mode
- Date
- Time
- Length
- The file's owner (if -q is present)
- Name

After this, the main function initializes three counter variables ($dirCount, $fileCount, and $sizeTotal) to zero and uses a foreach loop to iterate each path specified by the -path parameter. Inside the foreach loop, the function uses the switch statement to decide what to do with the results from the get-providername function. If the provider is FileSystem, the function uses the Invoke-Expression cmdlet to execute Get-ChildItem with the current path and the pipeline, then pipes the result to a ForEach-Object script block.

Inside the ForEach-Object script block, the main function checks for the -bare parameter. If the parameter is missing, the function invokes the formatted string expression it created earlier. If the item isn't a directory (i.e., if the item's Attributes property doesn't have the Directory bit set), the function increments the $fileCount and $sizeTotal variables; otherwise, the function increments the $dirCount variable.

Alternatively, if the -bare parameter is present, the main function only outputs the item's Name or FullName property (based on the $nameField variable). If the path isn't in the file system or if it doesn't exist, the main function uses the Write-Error cmdlet to output an error message and continues to the next path in the foreach loop.

After the ForEach-Object script block finishes, the main function again checks for the -bare parameter. If -bare is missing, the function outputs a formatted string containing the $fileCount, $sizeTotal, and $dirCount variables if either the $dirCount or $fileCount variables are non-zero.

It's All About Productivity

The limitations in PowerShell's Get-ChildItem cmdlet need not slow you down if you're used to Cmd.exe's dir command—let the D.ps1 script do the work for you. Put it in your Path and spend less time listing directories on your system.

InstantDoc ID 101900

Bill Stewart
(bill.stewart@frenchmortuary.com) is the systems and network administrator for French Mortuary in Albuquerque, New Mexico.

How will you manage your growing SharePoint environment?

Patch together a dozen products from a dozen vendors?

Hire a team of developers and consultants?

Get more SharePoint Admins?

Get DocAve®

One Platform for Comprehensive Backup, Disaster Recovery, Administration, Replication, Archiving, Compliance, and Migration for Microsoft® SharePoint.

DocAve by AvePoint® - Unleashing the power of SharePoint™

Find out why DocAve is the most award-winning solution of its kind
Download a FREE trial at: www.avepoint.com/unleash

AvePoint®

Office & SharePoint PRO
officesharepointpro.com

8 Points to Consider Before You Implement SharePoint

Make sure your SharePoint platform will perform well and be scalable

by Alan Sugano

So you're sold on the idea of using SharePoint in your office. When implementing SharePoint, what do you need to consider for a successful implementation? For the best performance and scalability, you need to consider:

1. Which SharePoint version will best meet your needs
2. The size of your first portal
3. Whether you want to use a 32-bit or 64-bit platform
4. Whether you want to use virtualization
5. Whether you need a high-availability solution
6. How you want to configure your SharePoint farm
7. How you want to back up your SharePoint platform
8. How you want to restore your SharePoint platform if a disaster strikes

1. SharePoint Versions

SharePoint comes in five versions:

- Windows SharePoint Services 3.0 (WSS 3.0)
- Microsoft Search Server 2008 Express
- Microsoft Office Forms Server 2007
- Microsoft Office SharePoint Server 2007 (MOSS 2007) with the Standard CAL
- MOSS 2007 with the Enterprise CAL or for Internet Sites

Determining which version to purchase can be a little confusing, so I'll summarize the key features of each version.

WSS 3.0 is a free download (technet.microsoft.com/en-us/windowsserver/sharepoint/bb400747.aspx) for users who have Windows Server 2008 or Windows Server 2003. WSS 3.0 is a fully functioning portal. It includes the Standard Site Templates and Web Parts and integration with Microsoft Office 2007. When you install MOSS 2007 (Standard or Enterprise) all the features in WSS 3.0 are included.

Search Server 2008 Express provides enterprise search capabilities for users of WSS 3.0 without requiring them to purchase the full version of MOSS 2007. With Search Server 2008 Express, users can search enterprise content sources and extend search capabilities with iFilters. It includes an improved relevance algorithm that's optimized for enterprise searches. It's available for free download at www.microsoft.com/enterprisesearch/en/us/search-server.aspx. All the features in Search Server 2008 Express are included with MOSS 2007 (Standard or Enterprise).

Office Forms Server 2007 lets users deploy forms created in Office InfoPath 2007 (available separately) on a SharePoint portal site and centrally manage those forms using Office InfoPath Forms Services. Microsoft released Office Forms Server 2007 to allow users of MOSS 2007 with the Standard CAL to use InfoPath forms without having to purchase MOSS 2007 with the Enterprise CAL. All the features in Office Forms Server 2007 are included in MOSS 2007 with the Enterprise CAL.

MOSS 2007 with the Standard CAL includes everything in WSS 3.0 and Search Server 2008 Express. It also includes Site Directory, Site Manager, Social Networking Web Parts, RSS feeds, user profiles and the Profile Store, audience targeting, Document Management Site Templates, Enterprise Site Templates, integration with Microsoft Information Rights Management, single sign-on (SSO), and other features. It doesn't include the ability to deploy InfoPath forms on the SharePoint portal.

MOSS 2007 with the Enterprise CAL includes everything in MOSS 2007 with the Standard CAL. In addition, it includes business intelligence (BI) features, which let you integrate data from external data sources such as ERP applications and other line of business (LOB) applications. You can integrate any database that's supported via an ADO.NET connection. It includes integrated Data Connection Libraries that centrally store approved connection strings to external data sources. It includes Excel Services, which lets users share BI information in Excel spreadsheets through a browser. With Excel Services, users can display charts, tables, pivot tables, dashboards, and scorecards created in Excel workbooks without any custom development.

For a complete listing of the features in the SharePoint versions,

go to office.microsoft.com/en-us/sharepointtechnology/FX101758691033.aspx. Note that regardless of the SharePoint version, you must store the SharePoint data on a back-end database server. With WSS 3.0, you can use the Windows Internal Database (which is also known as the Microsoft SQL Server 2005 Embedded Edition), but most people use either SQL Server 2008 (Standard or Enterprise Edition) or SQL Server 2005 (Standard or Enterprise Edition).

2. Portal Size

It's often difficult to predict how a SharePoint portal will be used. You might have grand plans for the portal only to find out that it gains little acceptance. Conversely, you might anticipate that it really won't catch on only to find extremely heavy traffic, with the portal struggling to keep up with the demand. In my experience, the best implementations start off small and grow as needed. The development cycle is a little different for portals because most items can be quickly changed and modified. For that reason, I strongly suggest using a prototype approach for any SharePoint project, regardless of the portal's ultimate size. Create a few sites, obtain feedback from users, make the necessary modifications, and repeat.

Some of the most successful implementations I've been involved with are projects that involve some type of catalyst, such as a portal being developed for a new store or a portal for a complex project that involves many players. This type of implementation is highly effective because users are highly motivated to get the maximum benefit out of the portal. It's vital that the SharePoint site becomes the final authority for these types of projects and that all key project players agree to post vital information on the portal. Once the information on the portal reaches a "critical mass" for a project, you're well on your way to successful SharePoint implementation. Once the users realize the potential power of SharePoint, they're more accepting of using SharePoint in other business areas.

One development approach is to develop the all-encompassing SharePoint site that's all things to all end users. In this situation, end users often get overwhelmed with the site and it might not fit their needs. This makes the SharePoint site a very difficult sell to end users, and the portal often goes unused. It's much better to start small and simple. Prototype and grow the portal as necessary.

3. 32 bit vs. 64 bit

Unless you have a compelling reason to install 32-bit SharePoint servers, consider using an x64 platform for both the front-end and back-end database servers. If you plan to integrate BI with your portal, you might need to install a 32-bit server for compatibility. For example, Microsoft Dynamics GP requires a 32-bit SharePoint server to integrate BI into a SharePoint site. However, x64 support is planned in the future.

One primary benefit of an x64 platform is scalability. With the 32-bit platform and the standard edition of Server 2008 or Windows 2003, you can address only 4GB of memory. With an x64 platform and the standard edition of Server 2008 or Windows 2003, you can address 32GB of memory. Scalability is especially important in environments in which you're unsure how big the portal will grow. The x64 platform has a greater capacity to handle a larger number of users combined with larger portal sites. With the x64 platform, you can somewhat compensate for a slower disk subsystem by adding more memory to the front-end or back-end servers, because this extra memory will cache disk information, providing better overall performance and reducing the load on the disk subsystem.

4. Virtualization

Virtualization lets you run multiple virtual servers on a single hardware host. For a small single front-end/back-end SharePoint server farm, virtualization is a good solution because of reduced hardware costs and better fault tolerance, but what about large installations? Virtualization of large SharePoint farms is also possible. Consider the following items when virtualizing your SharePoint environment:

- *Virtualization platform.* Although you can use free virtualization products that run on top of a general purpose OS (e.g., VMware Server, Microsoft Virtual Server 2005), I recommend that you use a hypervisor (e.g., VMware ESX Server, Microsoft Hyper-V) for the best performance. In my experience, hypervisors' performance is significantly better than that of free virtualization products. In addition, with hypervisors, you get significantly higher (sometimes double) consolidation rates of virtual servers per hardware host. You take a minimal performance hit (around 4 percent) for running a virtual machine on a hypervisor versus running that same machine on dedicated hardware.
- *Load balancing.* If you plan to load balance front-end servers in a virtual environment, make sure that the front-end servers are on different hosts. If you put the front-end servers on the same host, you'll probably take a performance hit rather than experience a performance gain and you won't gain any fault tolerance.
- *Memory limitations.* Both ESX Server and Hyper-V let you allocate up to 64GB of memory to a virtual server guest. Unless you're running an extremely large database server, this should be enough memory for most SharePoint database servers. Free products such as VMware Server and Virtual Server 2005 have a maximum of 3.8GB of memory per virtual server guest, which can be limiting even for a small SharePoint farm.
- *Anticipated CPU load.* SharePoint farm servers have a potential for heavy CPU loads from several sources: SSL sessions, virus scanning, stored procedures, and farm crawling. Some virtualization platforms like ESX Server let you reserve a number of CPU cycles for a specific virtual server guest. If you anticipate heavy SSL traffic and require load balancing on your front-end servers, consider using a dedicated SSL accelerator such as an F5 Network BIG-IP appliance to reduce the CPU load on your front-end servers. In a virtual world, don't rely on additional virtual CPUs to increase performance. Increasing the number of CPUs from one to four on a virtual server guest will yield marginal gains of approximately 10 percent. Hypervisors do a pretty good job of allocating resources to the host's CPUs. In general, you'll get better performance by reserving CPU cycles for a virtual server guest rather than allocating more CPUs to a guest.
- *Snapshots.* One nice feature of ESX Server and Hyper-V is the ability to take virtual guest snapshots. You can take snapshots of the SharePoint server farm before any major changes (e.g., service pack installa-

tion, major site upgrade) to the portal. If anything goes wrong when the changes are being implemented, you can revert back to the state of the farm before the changes. If everything goes smoothly, you can incorporate the changes into the virtual server. Snapshots typically take less than a minute to complete, making them significantly faster than even an incremental backup. Be aware that snapshots can quickly eat up space on the host. Taking a snapshot of a virtual server guest creates a delta file that records all the changes to the virtual server guest. When big changes are made to a virtual server guest that has a snapshot, it's not uncommon to see the delta file grow larger than the original virtual server disk file. For that reason, use snapshots sparingly and make sure you have plenty of free disk space available on your virtual server host.

- *x64 guest support.* If you plan to run x64 virtual server guests, you need to verify two factors: The virtualization platform must support x64 guests (ESX Server and Hyper-v have x64 guest support), and the virtual server host's BIOS and CPU must be capable of x64 virtualization.
- *Disaster recovery.* If you've been unfortunate enough to go through the task of recovering a SharePoint farm, you know that it's difficult and painful, even with good backups. If your SharePoint farm is running on a virtualized platform and you have image backups of your virtual servers, the recovery process is significantly simplified. I suggest that you take image backups of your virtual server guest at least once a week along with performing traditional full or differential backups during the week. Virtual server image backups involve taking a snapshot of the virtual server guest, backing up the virtual server disk file, then deleting the snapshot. If you have the virtual server disk images backed up, the recovery process is significantly simplified. To restore the virtual server on a different host, you just need to install the hypervisor on the new hardware, install the backup software, install the backup agent on the virtual server host, and restore the virtual server disk images. After you start the virtual server guests, you might need to restore the latest full or differential backup. Because virtualization creates a hardware-agnostic platform, you can restore these virtual server guest images on a different virtual server host running the same virtualization platform without any problems. If you have x64 virtual server guests, make sure your new host is capable of hosting x64 virtual server guests.

5. High Availability

A comprehensive discussion of high availability is beyond the scope of this article. However, here are a few guidelines when considering a high-availability solution. If your SharePoint farm must be highly available, consider either Microsoft or VMware clusters. Clusters typically involve shared storage on a SAN with two or more cluster nodes. Clusters are designed to automatically fail over to a different host in the event of a hardware failure. Microsoft clusters are typically single-application clusters, such as a Microsoft Exchange or SQL Server cluster. VMware clusters often are multiple-application clusters, where different applications reside on the same cluster. VMware clusters offer better granular failover capabilities compared to using Microsoft clusters. Clusters are expensive. An iSCSI SAN typically starts at $30,000, and a Fibre Channel SAN starts at $50,000. That's just for the SAN—you still have to purchase the server nodes and software. The easiest way to justify the cost of a cluster is to calculate the cost of downtime.

I typically start considering high-availability solutions for companies that have 250 or more users. I have installed clusters for companies that have fewer users. For example, I had a client that managed a hedge fund that estimated the cost of downtime at $20,000 per minute. Although there were only 30 users in the office, the client decided to implement a cluster because of this high downtime cost.

6. SharePoint Farm Configuration

Many factors must be considered when designing the optimal SharePoint farm configuration for your company's SharePoint portal. Here are a few items to consider when designing your farm:

- *Internet access to the portal.* What is the anticipated traffic from the Internet? Make sure to take into account not only your Internet connection line speed but also the current peak and average utilization of your Internet connection. If you anticipate heavy usage from the Internet, you might need to increase your Internet bandwidth. When accessing a SharePoint site from the Internet, I consider SSL connection mandatory. Multiple SSL sessions can place a significant load on the SharePoint web server. If you anticipate more than 50 concurrent sessions, consider using a dedicated SSL load-balancing appliance with two or more front-end servers for fault tolerance. This appliance will reduce the CPU load on the web server and often do a much better job of load balancing compared to Microsoft's Network Load Balancing (NLB) because the appliance will take into account actual traffic volume rather than connection counts. SSL load-balancing appliances usually provide an SSL proxy and packet inspection of the SSL traffic, greatly increasing the security on the SharePoint site. If the portal will be accessed primary from the Internet, consider placing the SharePoint farm in a co-location facility or hosted SharePoint services facility.
- *Dedicated servers for SharePoint roles.* If you anticipate heavy usage of the portal for searches, web services, document conversions, or Excel calculation services, consider dedicating a server to each server role in which you're expecting heavy usage. For fault tolerance,

consider using two or more servers for each role for high availability.

- *Database servers.* If your site is extremely large, you might want to distribute your logical SharePoint site across two or more database servers.

One of the most common SharePoint farm designs is a single back-end SQL Server database server with a single front-end server. The front-end server manages the areas of central administration, web services, document conversions, Excel calculation services, searches, and incoming email.

If you're using virtualized servers on a single virtual server host for a SharePoint farm, it doesn't make sense to break out the different SharePoint server roles on multiple servers. There is one exception: You should separate the database server from the rest of the SharePoint server roles primarily for security reasons. If you're running virtualized servers for your SharePoint farm and you need high availability and load balancing, make sure you don't have virtualized servers with the same roles running on the same host server. For example, if you want high availability and load balancing for your SharePoint web servers in a virtual environment, make sure that each virtual server is running on a different host. Placing two virtual servers on the same host won't increase fault tolerance because a hardware failure on the host server will cause both virtual servers to go down. In addition, placing two virtual servers on the same host will probably hurt rather than help performance. For comprehensive information about SharePoint farm design considerations, download the free book *Planning and Architecture for Office SharePoint Server 2007* at technet.microsoft.com/en-us/library/cc262757(TechNet.10).aspx.

7. Backups

If you're using a SQL Server backup agent, you can somewhat protect a SharePoint installation by either backing up the SQL Server database or dumping the SQL Server database to a file that later gets saved offline. You should back up all the other servers in your SharePoint farm as well. For larger environments that use a SAN, you can take snapshots of the SAN and save them to Just a Bunch of Disks (JBOD) to get around backup time constraints. However, online backups are vulnerable to virus outbreaks and other malware attacks that can potentially leave them useless, so it's important that you copy the snapshot backups to some type of offline media as well.

Most of the major backup software programs now support MOSS 2007–specific backup agents. The advantage of SharePoint-specific backup agents is they offer granular restore and are usually multiserver-farm-aware. Even if you're really good with SQL Server restores, granular restores without a SharePoint-specific backup agent can be tricky. I've found that restore requests usually aren't for the entire SharePoint site but rather for specific subsites or specific content on the portal. This is when these backup agents justify their cost. Although you're somewhat protected with MOSS 2007's Recycle Bin feature, I've run into situations when I still needed to perform a granular restore.

If you have mission-critical data stored on the portal, I suggest purchasing and using backup software that has a MOSS 2007-specific backup agent. I recommend that you either perform a full backup once a week with differential backups during the week or a full daily backup of your SharePoint portal.

8. Disaster Recovery

If you work for a publicly traded company that must be Sarbanes-Oxley (SOX) compliant, it's important to prove you can recover from a disaster and prove how quickly you can recover. If you've had the unfortunate experience of recovering your SharePoint site after a major hardware failure or disaster, you know it can be challenging. Running a multiserver farm only complicates the restore process. Consider the steps to recover a simple two-server SharePoint farm:

1. Purchase new hardware.
2. Install Server 2008 or Windows 2003 on the database server.
3. Install the backup software.
4. Catalog the tape on the backup server.
5. Install the backup agent on the database server.
6. Restore the programs (including SQL Server) on the database server.
7. Restore the databases on the database server.
8. Install Server 2008 or Windows 2003 on the front-end server.
9. Install the backup agent on the front-end server.
10. Restore SharePoint on the front-end server.
11. Test.

If your SharePoint farm is running virtualized servers, it greatly simplifies the process if you have the virtual server guest images backed up weekly with a traditional backup performed during the week. Consider the following steps using ESX Server as the virtualization platform:

1. Purchase new hardware.
2. Install ESX Server on the host server.
3. Install the backup software.
4. Catalog the tape on the backup server.
5. Install the backup agent on the ESX Server host.
6. Restore the SharePoint farm servers on the ESX Server host and start them.
7. If necessary, restore the latest full or differential backup on the servers. Optionally, restore the latest full or differential backup on the database server.
8. Test.

There are also two major advantages when using virtualization for disaster recovery: There's significantly less administrator involvement during the restore process, and restoring to different host hardware doesn't complicate the process. When using virtualization for disaster recovery, you should be able to reduce the recovery time by at least half compared to restoring the servers on bare metal.

Take the Time

To implement a SharePoint platform that's optimized for your company, you need to consider many factors. Taking the time to address each factor will help ensure your portal performs well and is easily scalable.

InstantDoc ID 102028

Alan Sugano
(asugano@adscon.com) is the president of ADS Consulting Group, which specializes in networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

- Smartphones
- SharePoint
- Adobe Flash
- Training and Certification

Adobe Brings Flash to the Living Room

Adobe announced that it's extending its popular **Flash** platform, which is primarily used to deliver digital video over the web, to now deliver video to the living room via TV sets, Blu-ray players, and other set-top boxes. The company has signed agreements with a wide variety of consumer electronics companies, many of which will ship Flash-based products in the first half of 2009. Notably, the Flash Platform for the Digital Home supports HD quality video as well as rich, connected hybrid applications, without requiring a web browser. According to Adobe, customers utilizing products based on this technology will be able to seamlessly switch between HD video content delivered via traditional TV signals and the web. To learn more, visit www.adobe.com.

Certification Training Flash Cards

Looking for a testing edge before your next certification exam? Maybe flash cards will hold the key. InformIT offers dozens of online flash card sets that offer questions from previous certification exams. You can sort the questions randomly or test based on your weak points, and compare your answers to the recommended answers. Then you rate yourself, and the flash cards (which are really a sortable online quiz) tell you if you passed or not. The biggest downside is the risk that you will simply learn all of the questions, rather than build a depth of understanding so that you're ready for anything come exam day. A set of flash cards, which averages 300 questions, costs about $20–$25. To learn more, visit www.certflashcardsonline.com.

Azaleos Unveils New SharePoint Services

Azaleos has unveiled **Azaleos SharePoint Services,** a new services offering aimed at helping IT pros monitor and manage their SharePoint infrastructures. Azaleos SharePoint Services is intended to provide IT pros with 24x7 remote managing and

PRODUCT SPOTLIGHT

Automate Management of Popular Smartphones

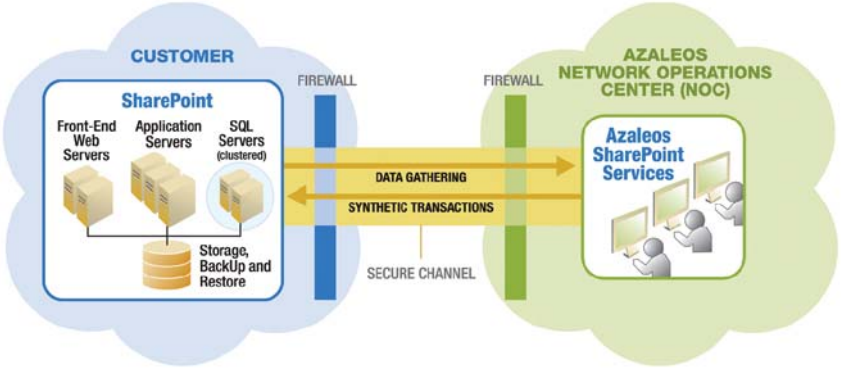
You've probably struggled with the inherent challenges associated with managing a mobile workforce. Do your mobile users complain that email is failing to reach their phones? Are they experiencing calendar-reconciliation problems? Do new phones have trouble establishing network connectivity? You have plenty of management policies in place for your servers and desktops, but what about those Research in Motion (RIM) BlackBerry, Apple iPhone, and Windows Mobile smartphones? They're proliferating at a wild clip, so how do you rein them in? The Radicati Group predicts there will be 600 million smartphones in the enterprise by 2011, so the problem certainly isn't going anywhere.

"Increasingly, we're seeing a 'consumeration' of the enterprise," says Ahmed Datoo, Zenprise's vice president of marketing. "And at the same time, today's economy is creating flat-budget IT departments that don't know how to tackle smartphone growth."

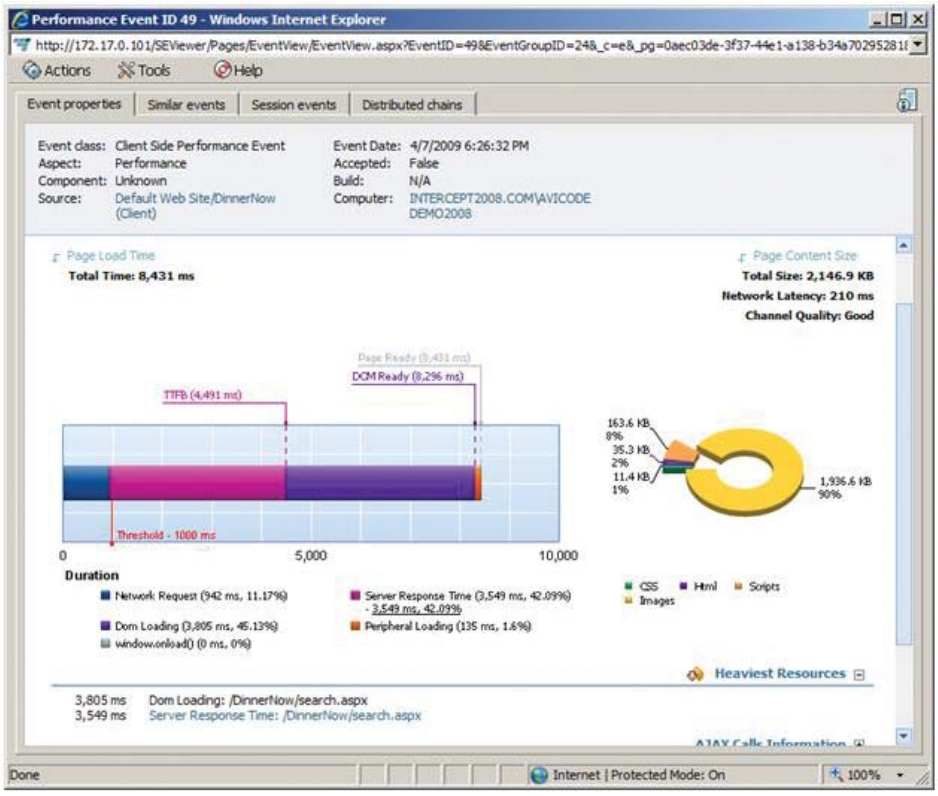
Zenprise's answer is to automate smartphone management, and it does so with its **MobileManager** platform. MobileManager has supported BlackBerry and iPhone deployments, and will now support Windows Mobile deployments. Through its use of automation, Zenprise MobileManager introduces a best-practices approach to finding and fixing user problems. Just as data-center automation introduced a new level of efficiency into provisioning and managing heterogeneous servers, automating mobile service management delivers a cost-effective way to support and manage complex, heterogeneous smartphone environments. This approach lowers mean time to repair, standardizes problem resolution, minimizes support calls, and improves overall productivity.

"Think of the TV show House," said Datoo. "You've got a bunch of smart doctors trying to diagnose illnesses. They go through initial tests and then secondary tests, all the while narrowing down to a smart diagnosis. That's what we're doing in MobileManager: We've automated 6500 troubleshooting processes so that kind of smart diagnostics and repair can happen behind the scenes. And that kind of service is unique in the mobile space."

Pricing begins at $35 per user for 1,000 users. To learn more, visit www.zenprise.com.



Jeff James | jjames@windowsitpro.com
Editor's Note: Send new product announcements to products@windowsitpro.com.



monitoring of Microsoft Office SharePoint Server (MOSS) installations. According to Azaleos, this new offering leverages some of their patented technology to remotely monitor thousands of points of relevant data from a customer's IT infrastructure, including data collected from MOSS, SQL Server, and Internet Information Server (IIS) as well as hardware, storage, and networking information. Azaleos' new SharePoint offering uses a virtualized architecture to deploy SharePoint Services, which the company claims provides better uptime, decreases energy costs, and reduces hardware requirements. Pricing begins at $15 per user/month. To learn more, visit www.azaleos.com.

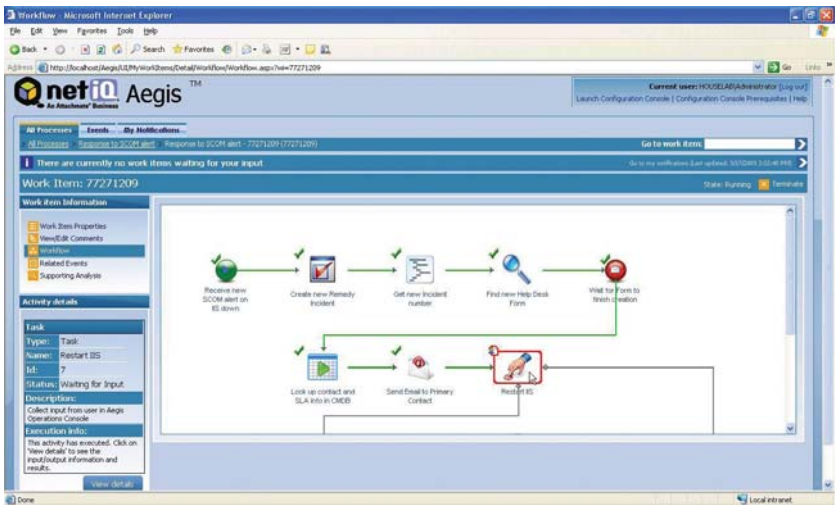
AVIcode Adds Client-side Monitoring to Intercept Studio

AVIcode has announced **Intercept uX,** a product that works on top of Intercept Studio to monitor sites from the client's viewpoint. According to AVIcode, only 30 to 60 percent of client performance can be measured at the server side. Intercept uX reports on factors like the time it takes to load JavaScript and images and correlates this information with server information. It can also detect JavaScript errors, even though client browsers don't usually report the errors, and it can monitor "Web 2.0" functions like AJAX calls.

Intercept uX works without installing anything on the clients and doesn't require changes to your pages' code. It injects the monitoring code from your application server. The product works for both intranet and Internet sites, and end users won't notice anything. For now, the product requires .NET server. Intercept uX is $7,995 if purchased with Intercept Studio, and $9,995 if purchased as an upgrade. Visit www.avicode.com for more information.

NetIQ Aegis Adding SCOM Support

NetIQ released an adapter for **Aegis** that supports Microsoft System Center Operations Manager (SCOM). Aegis is an IT process automation package, and adding SCOM integration should add value for current SCOM users. Under SCOM, you get alerts about things like a server being down or a site being unavailable. Aegis can correlate information from alerts, events, and other sources, reducing the number of events reported to IT staff. Aegis packages relevant information before sending an IT pro an email, who can then reply to the email and authorizing action, such as restarting a server. The alerts also provide a link that goes to web pages with charts and data about the reported problem, allowing an IT admin to manage systems from any Internet connection, or even smartphones. You can use Aegis to automate responses to common events or automatically create work orders. To learn more, visit www.netiq.com.



Group Policy Management Tools

Three computer management problems, three different third-party solutions

by Eric B. Rux

Ever since two PCs were first connected to one another in a business environment, systems administrators have been trying to find easier ways to manage networked computers. In Windows 2000 Microsoft introduced group policies that laid a foundation for PC management that's still in use today. In this article I review three Group Policy products that all play a different role in how you manage the computers on your network. Two of the products either use or integrate heavily with Group Policy, whereas the other product relies on a custom solution.

BeyondTrust Privilege Manager

BeyondTrust Privilege Manager's aim is simple: to remove the requirement that users must be local administrators on their PCs in order to run software. This goal seems simple at first—until you actually try to accomplish it. In addition to not being able to run software, regular users can't change the time zone or run the built-in disk defragmenter utility. Privilege Manager lets you easily grant permissions on an application-by-application basis.

Installation. I followed the Privilege Manager Installation Guide PDF, which walked me through the simple installation procedure. You can install Privilege Manager on Windows Server 2003 SP1 or better, or on Win2K SP4. You need to install the program on the same machine that you use to edit Group Policy. Be sure to install the Microsoft .NET Framework 2.0, which you can download from Microsoft's website. Installation is fast, taking only a few minutes—and it doesn't require any user intervention. The installation is also clean; it doesn't add any desktop shortcuts or Start menu items. Instead, Privilege Manager adds itself into Group Policy Object Editor as a Group Policy extension, as Figure 1, page 44, shows. Privilege Manager comes in both a 32-bit and a 64-bit version. Of the three solutions that I tested, Privilege Manager was by far the easiest to install and configure.

Figure 1: Privilege Manager integration with Group Policy Object Editor

In addition to the administration portion of Privilege Manager, you must install a client for each PC that you want to manage. Because the client is in MSI format, you can easily deploy it through Group Policy. The client also comes in both 32-bit and 64-bit versions.

Configuration and use. Configuring a new Privilege Manager policy to allow users to run software is just like creating a new Group Policy setting. The new policy can be applied to users and computers during computer startup or user logon, or at 90-minute intervals. I started with a new Group Policy setting and navigated to the Group Policy Object (GPO) extension called Computer Security, which is added when Privilege Manager is installed. Next, I right-clicked and created a new Privilege Manager policy. You can choose from nine types of rules, including Path Rule (allow an application based on its path); Hash Rule (allow an application based on its hash); and rules for folders, MSI files, and certificates. An "everything rule" (called a Shell Rule) lets users run any application they want, while keeping a strict audit on the activity. This rule is useful for "power users" (e.g., developers) whose application-running privileges can't be restricted, but who need to be reminded that they are responsible for what happens on their machine. You can even set a rule to prompt the user to enter a justification for running an application.

Privilege Manager's configuration and capabilities are flexible. For example, you can create a Self-Service Installation Point, which is a read-only network share with a Folder Rule applied to it and that includes software you want users to be able to install. If a user requests a specific application, you can simply drop the setup files into the network share, and the user can then install the application.

Although you can set up a rule for any application that you want users to be able to run, Privilege Manager also has some built-in rules for common tasks. For example, you can give users permission to change their time zone, run a disk defrag, set the power options, or configure accessibility options.

Sometimes the exact process and variables a program uses aren't obvious. For these situations, Privilege Manager includes a cool troubleshooting tool called Policy Monitor (PolMon.exe). Policy Monitor displays the specific commands used when a user tries to change the time or defragment the hard drive. If you have a custom application that you need to give a user elevated privileges to, this handy tool will give you the information you need.

Each Privilege Manager rule can be filtered by an unlimited number of rules that you can define. For example, you can filter by computer name, IP address range, OS, user or security group, and approximately 22 other filter objects. If these rules don't meet your needs, you can even write your own Windows Management Instrumentation (WMI) query.

Privilege Manager makes the daunting task of removing users from the local administrators group much easier. If your security policy requires this change, consider using Privilege Manager rather than trying to tackle the job yourself.

BeyondTrust Privilege Manager

PROS: Easy to give users elevated privileges on an application-by-application basis; simple installation

CONS: Cost per seat might put this handy solution out of reach for some budget-minded companies

RATING: ◆◆◆◆◇

PRICE: $37.20/seat (includes Upgrade Assurance and Premium Support)

RECOMMENDATION: Privilege Manager is a good solution if you don't have time to manually research how to relax the folder and registry permissions so that your users don't have to be local administrators.

CONTACT: BeyondTrust • 603-610-4255 • www.beyondtrust.com

Policy Commander

Policy Commander lets you secure the computers on your network, based on industry standards such as HIPAA. Email alerts and reports help you keep track of your computers' security status.

Installation. Policy Commander has four components (not including the client agent). These components can be installed on one central server or workstation, or separated onto multiple machines for extremely large organizations. For my tests, I installed everything onto the domain controller (DC).

First you must install the .NET Framework 2.0. Next, install the setup.exe file, which will prompt you for the license serial number and the options you want to install. Unless you're running Microsoft SQL Server 2000 SP3 or later, the setup routine will automatically install and configure SQL Express.

Installation took about 10 minutes but went off without a hitch (after a brief call to New Boundary Technologies' technical support). After the installation completed, a Help window opened that explained how to use the product.

Configuration and use. My first configuration task was to set the polling interval. For this evaluation, I chose to poll continuously.

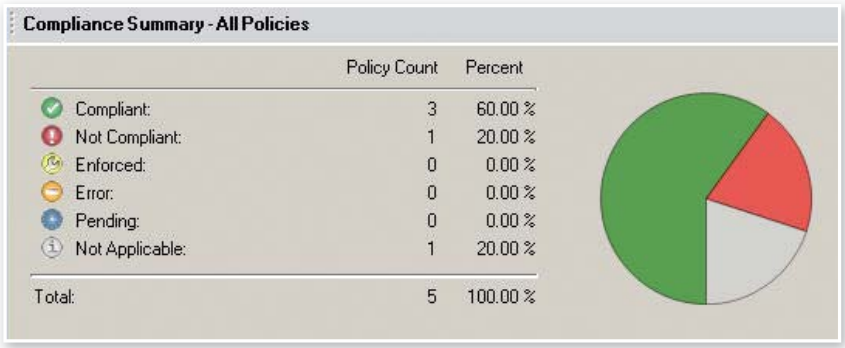


Figure 2: Policy Commander report and graph

In a production environment, however, you would poll much less often—maybe hourly or daily, depending on your security requirements.

Next, I added the computers I wanted to use Policy Commander to manage. You can add computers manually through the console or with a Group Policy logon script. The Group Policy method ensures that all new PCs added to the domain are automatically added to the Policy Commander console. Because the console method requires the client PC to reboot, you should let users know before pushing the client out to everyone.

Once the client was installed, I was ready to jump in and start locking down the PCs. Policies can be assigned to individual computers or to computer groups within Policy Commander. There are two kinds of groups: organizational groups and configuration groups. Organizational groups are static and let you organize the computer structure in any way that makes sense to you. Configuration groups are dynamic—computer objects are added and removed automatically, based on specific criteria. Some built-in configuration groups are Microsoft Office Version, OS Version, and Security Groups. You can also build your own configuration group based on values such as free disk space, registry value, etc. You can even build these groups based on a WMI value. For example, if you wanted to deploy a policy to all the computers in the accounting department, you could create an organizational group and manually move the PCs you wanted the policy to apply to. Alternatively, you could create a configuration group that dynamically creates a group of PCs in the accounting department based on a specific rule.

After you define how you want to group your computers, you can assign policies to them. Policy Commander includes 12 predefined policies to get you started, or you can create your own policies. Figure 2 shows Policy Commander's graphing and reporting capabilities, which your manager or compliance auditors will likely be interested in. This figure shows a total of five policies, three of which are compliant and being enforced, one of which isn't in compliance, and one that isn't applicable. To determine which machines are out of compliance, you can select the Policy Commander console's Policy Compliance tab. In addition, you can receive email alerts about PCs that have fallen out of compliance, so that you can take swift action.

If Policy Commander's 12 predefined policies aren't sufficient for your needs, you can use the Policy Editor to create your own custom policies. You can also download industry-standard policies from New Boundary Technologies' Policy Knowledge Base. For example, if you manage PCs in a hospital or medical environment, you might want to implement the HIPAA policies. Or, if you work in a military or other highly secure network, you might want to download the NSA security policies. Downloading and installing these policies is simple and automatic.

Policy Commander is extremely robust in how it filters and applies policies to computers in your Active Directory (AD) domain. Note that these polices aren't Group Policy settings—they are custom solutions that use an agent on each computer. If your SOX, SAS-70, or HIPAA auditors are hounding you for proof that your network is secure, then Policy Commander is worth a look.

Policy Commander

PROS: Downloadable security policies take the guesswork out of securing your PCs

CONS: Must have the client installed for the settings to take effect; need to create a Group Policy setting to install the client as soon as the computer object is added to the OU

RATING: ◆◆◆◆◇

PRICE: $30/seat (Power Management–only version also available for $15/seat)

RECOMMENDATION: Policy Commander is worth a look if your SOX, SAS-70, or HIPAA auditors are hounding you for proof that your network is secure.

CONTACT: New Boundary Technologies • 800-747-4487 • www.newboundary.com

GPOADmin with NetPro NetControl

I previously reviewed an earlier version of **GPOADmin** in "3 Tools to Manage Group Policy" (November 2007, InstantDoc ID 97228). Back then the product was just called GPOADmin (before Quest Software acquired NetPro Computing). NetPro's GPOADmin had one missing component compared with the competing products at the time (NetIQ's Group Policy Administrator and ScriptLogic's Active Administrator): The product lacked a Group Policy repository. When you made changes to Group Policy settings, you were actually changing the production objects. The new version of GPOADmin has an offline repository, as well as other useful features.

As in my previous review, I ran GPOADmin through a scenario that you might see in a typical large company trying to manage Group Policy changes. I created the following Group Policy change-management process, then used GPOADmin to implement Group Policy within the process:

1. A request is made to create or alter Group Policy.
2. The request is reviewed by peers and tested in a lab.
3. Implementation is approved.
4. The original GPO (if applicable) is backed up for rollback purposes.
5. An offline GPO is created, edited, then verified by peers.
6. The approved GPO is linked to the appropriate organizational unit (OU), and the old GPO is unlinked, if applicable.
7. Verification that the new GPO is in production is made.
8. Changes made to GPOs are audited periodically to ensure that the rules are being followed.

Installation. Like Privilege Manager

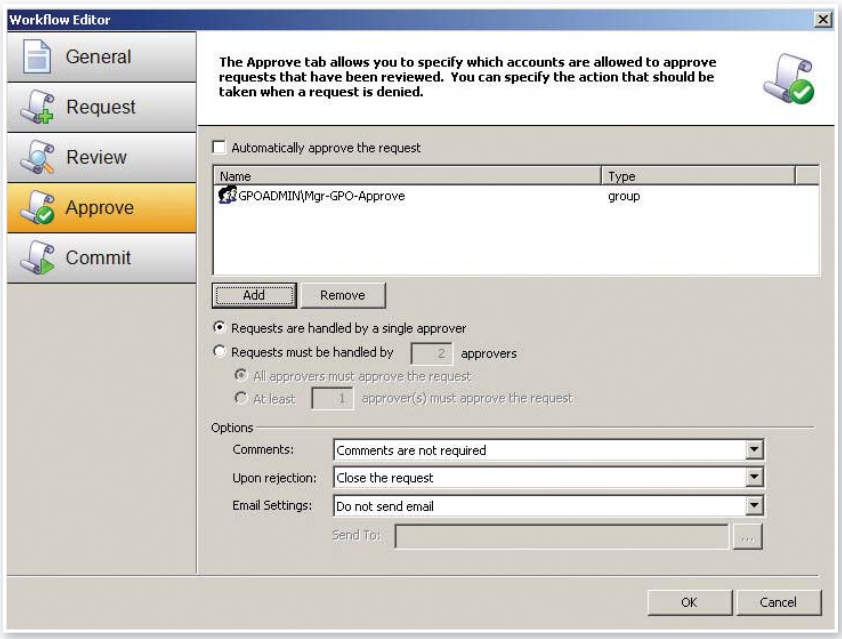


Figure 3: GPOADmin's workflow approval process

and Policy Commander, GPOADmin requires the .NET Framework 2.0. In addition, GPOADmin requires Microsoft's free Group Policy Management Console (GPMC) and either Microsoft SQL Server or SQL Server Express. To install GPOADmin, you need to invoke four separate installation routines: NetPro Server, NetPro Console, GPOADmin Extensions, and the NetPro GPOADmin tool. The NetPro Server installation prompts you for a license file and for the name of the SQL Server machine that will store the Group Policy repository. I had some trouble with the license file that I was given for the review, as well as some questions about the many applications that had to be installed and configured. A call to Quest Software tech support quickly resolved my problems.

Configuration and use. After the product was installed, I opened NetPro NetControl and finished the configuration process, specifying the database, versioning, cloaking, offline editing, and logging (all features that were missing from the product when I reviewed it two years ago). The interface walked me through each process and even helped me create a connection to the SQL Server machine and create a new database.

GPOADmin is an extension of Microsoft's GPMC, so you invoke this familiar tool to create or edit a Group Policy setting. When you click the domain, a window on the right-hand pane shows four tabs titled *Access and Monitoring, Reports, Deleted Items,* and *Lineages.* A fifth tab called *Standard* simply shows the GPMC window you'd see if GPOADmin weren't installed.

The *Access and Monitoring* tab lets you compare two or more Group Policy settings. This feature is useful in troubleshooting when one GPO is performing as you expect, while another isn't. The *Reports* and *Deleted Items* tabs are self explanatory, although their features are welcome additions to the standard GPMC. The *Lineage* tab helps you roll out new Group Policy settings in stages, as well as quickly roll back GPOs that don't work as expected. This new functionality fulfills steps 4 through 8 in the Group Policy change-management process that I outlined earlier. But what really makes GPOADmin an enterprise-level product is the workflow functionality included in the NetControl portion of the product.

Workflow in NetControl consists of four steps: Request, Review, Approve, and Commit. Permissions for these four steps are set in the NetControl application, which Figure 3 shows. You can give users or groups permission to request, review, or approve Group Policy settings. When it comes time to commit, you can set GPOADmin to immediately commit the policy after it's approved, or wait until a specified time (e.g., after work hours). Once the GPO is committed, an email message can be sent to a user or distribution group to let them know that the new policy was applied.

Other useful features in GPOADmin are Cloak and Lock. Cloak lets you hide a Group Policy setting that you aren't yet ready for anyone else to see. Lock prevents other administrators from changing your Group Policy setting. Even though these features are unique to the GPOADmin GUI, they both use security groups as the backbone of their functionality. If another administrator uses Windows Server's built-in GPO editing tools, these rules will still apply and the Group Policy settings will remain protected.

GPOADmin with NetPro NetControl

PROS: New workflow functionality makes it a true enterprise-class product; easily fit into my new GPO process

CONS: Complex installation

RATING: ◆◆◆◆◇

PRICE: $12/enabled user account

RECOMMENDATION: Use this product to create a Group Policy workflow approval process.

CONTACT: Quest Software • 800-306-9329 • www.quest.com

Different Problems, Different Solutions

Managing network computers is a full-time job. Privilege Manager, Policy Commander, and GPOADmin each fill gaps that exist in a standard Windows installation. If you need to remove users from the local administrators group, or if you need to lock down all your PCs and be able to prove it with online reports, or if you need to create a Group Policy workflow approval process, you should take a look at these three products. One of them just might be what you're looking for.

InstantDoc ID 102125

Eric B. Rux

(ebrux@whshelp.com) is a contributing editor for *Windows IT Pro* and cofounder of WHSHelp.com. He writes a column at svconline.com/connectedhome and teaches the Microsoft Certified Systems Administrator (MCSA) program at a tech college.

Windows Server Intrusion Detection Products

Your network isn't safe unless you have something in place to stop intruders. This guide shows your options to do the job.

by Lavon Peters

Good security practices help protect your network against attacks by intruders, malicious applications, and a host of other threats. Part of a successful security plan is having the right products in your arsenal—a simple firewall and antivirus product won't suffice. To fully protect your network, you need intrusion detection and prevention coverage. Intrusion detection systems (IDSs) monitor for open ports on your network to detect security vulnerabilities that leave your systems open to attack. Intrusion prevention systems (IPSs) go even further, actually preventing attacks from occurring.

A multitude of IDS and IPS products exist, ranging from software and services to appliances. For this Buyer's Guide, we focus on IDS and IPS software and services. In addition, many solutions are free—which we highlight in the accompanying table.

To determine which product is right for your environment, consider the following aspects of intrusion detection and prevention. Then, consult the Buyer's Guide table on page 48 for an overview of products.

Detection/Prevention Methods

Methods of intrusion detection vary widely. The most common type of intrusion detection is the rule-based (or signature-based) method. This type of detection compares an attack signature to network traffic to identify potential threats. Other intrusion detection methods include network behavior analysis, event log monitoring and reporting, database auditing, baseline snapshot comparison, pattern recognition, and heuristic analysis.

User Input and Configuration

In choosing an IDS or IPS, you might want to consider how much user input is required (or even possible). For example, does the program run unattended, or does it require user input? Are scans customizable—that is, do they adhere to a predefined policy, or can you apply user-created rules? You should also take into account how often the program is updated, and whether updates are automatic or user-scheduled. Update frequency can range from yearly to hourly, or even as needed in real time. Finally, do scans occur continuously, or only during scheduled times? Although for ease of use you might prefer an IDS/IPS product that runs out-of-the-box, for the best security protection you might want to be able to fine-tune the program to suit your environment and specific needs.

Management and Reporting

Even if you have the best IDS or IPS product imaginable, it's useless if you can't easily retrieve the information it gathers. Consider whether the program you're looking at offers centralized management, preferably through an easy-to-use console that provides configuration, monitoring, and reporting. Another criterion to evaluate is the product's reporting capabilities. For example, are reports canned or customizable? Also, how are reports provided (e.g., HTML, PDF, email)?

Virtualization

If your organization uses virtualization, as so many companies do these days, you need to determine whether the product you're considering supports and can run in a virtualized environment. Can the program run on a virtual machine (VM)? Can it scan VMs? And does it work with all virtualization platforms, or only one?

Go Forth and Detect

Evaluating all the aspects of intrusion detection and prevention will help you find the best product for your environment. Once you have an IDS or IPS up and running, you can sleep easier knowing your systems are safe from attack—or at least safer than they were without it.

InstantDoc ID 102109

LAVON PETERS (lpeters@windowsitpro.com) is a senior editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in security. She has worked as a technical editor since 1994.

WINDOWS SERVER INTRUSION DETECTION PRODUCTS

Company	Product	Price	Software or Service?	Supported Windows Versions?	Detection Method(s)?
AppliCure Technologies 800-584-4888 www.applicure.com	dotDefender dotDefender Monitor	Contact vendor for dotDefender pricing; dotDefender Monitor is free	Software for end users; SaaS for hosting providers	Windows Server 2008, Server 2008 64-bit; Windows Server 2003, Server 2003 64-bit For web servers: IIS 7.0, IIS 6.0	Pattern recognition, session protection, signature knowledgebase
Check Point Software Technologies 866-488-6691 or 650-628-2070 www.checkpoint.com	IPS Software Blade	$3,000	Software	Windows Server 2008, 2003	Firewall, signature-based detection, protocol RFC compliance checks, anomaly detection, brute-force detection, protection evasion avoidance, network usage control, Malicious Code Protector (inline executable code analysis checks), DoS prevention
ESET 619-876-5400 www.eset.com	ESET NOD32 Antivirus 4	From $40.99 per license per year, for 5-10 licenses, to $11.99 per license per year for 50,000+ licenses	Software	Windows Server 2008 (32- and 64-bit), 2003 (32- and 64-bit), 2000 Pro, 2000; Vista (32- and 64-bit); XP (32- and 64-bit)	Signature checking, firewall, behavior-based, antispam, antispyware
GFI Software 888-243-4329 www.gfi.com	GFI EventsManager	1-9 nodes for servers, €220.00 per node; 10-24 nodes for workstations, €22.00 per node	Software	Windows Server 2008, 2003, 2000; XP; SBS 2008, 2003	Event log monitoring
Ionx www.ionx.co.uk	Data Sentinel	$350 (volume discounts available)	Software	Windows Server 2003, 2000; XP Pro; NT 4.0	Comparison against baseline snapshot (file system and registry)
Lan-Secure www.lan-secure.com	Security Center	Lite Version, $999; Enterprise Version, price is based on number of nodes	Both	Windows 2008, 2003; Vista, XP	Behavior-based
Microsoft 800-642-7676 www.microsoft.com	Forefront Threat Management Gateway	Contact vendor	Software	Windows Server 2008 (64-bit)	Multiple methods, including stateful inspection firewall, application layer firewall, signature checking, and behavior-based vulnerability signatures
Safety-Lab www.safety-lab.com	Shadow Security Scanner	From $499	Software	Windows 7; Vista; XP; 2003, 2000	Database auditing, heuristic analysis
StillSecure 303-381-3800 www.stillsecure.com	Safe Access	Pricing ranges from $2,500 for 50Mbps of throughput to $15,000 for 4Gbps of throughput	Both	All	Stateful packet analysis, signature analysis, TCP stream reassembly analysis, protocol anomaly/behavior analysis, Layer-2 analysis, DoS/DDoS detection
Sourcefire 800-917-4134	SNORT	Free	Software	All	Rules-based with anomaly detection
	Sourcefire 3D System	Depends on configuration	Software	All	Rules, anomaly detection, network behavior analysis

	Runs Unattended?	Automatic or Manual Updates? How Often?	Customizable Scans?	Runs Continuoulsly?	Centralized Management?	Reporting Capabilities?	Virtualization Support?
	Integrates with the web server and runs when active HTTP traffic is processed	Automatic; every few months	Yes	Yes	Central management console for configuration, monitoring, and reporting	Predefined reports include executive, standard, and detailed; customized reports available; dashboard shows immediate system status	Yes
	Yes	Automatic or manual; weekly	Yes	Continuously, with optional detect-only mode, which sets all or some of the protections to detect but not block traffic so user can evaluate profile without disruption	Yes	Configurable, actionable monitoring; tracks events through detailed reports and logs (business–level views, multi–dimensional sorting, actionable event logs)	Yes
	Yes	Automatic; updates average 2-3 times/day; schedule is user customizable	Yes	Continuously or scheduled	Yes	Reports on scan results, threat results, firewall logs, event logs	Yes
	Yes	Manual	Yes	Continuously or scheduled	Yes	Through a free add-on report pack	No
	No	Manual; updates released as necessary or once per year	Yes	No	No	HTML, CSV, XML, email	Yes
	Yes	Manual; quarterly	Yes	Yes	Yes	HTML, SQL, email, SNMP, Syslog	No
	Yes	Continuously updated through signatures	Yes; customers can create application layer filters to extend the product	Yes	Yes	Built-in, centralized investigation through Forefront codename Stirling, and customizable through SQL Server	Yes
	No	Automatic or manual; daily	Yes	Yes	Yes	HTML, PDF, XML	No
	Yes	Automatic; as often as hourly	Yes	Yes	Yes	On-demand and automated scheduled reporting	Yes
	Yes	Manual; weekly	Yes	Continuously or scheduled	Third-party management	Third-party reporting	Yes
	Yes	Automatic or manual; weekly	Yes	Yes	Yes	Full-featured reporting engine	Yes

Top 10 Features

What to Look For in a Data Migration Solution

Migrate data more effectively and efficiently with these 10 tips. This handy reference guide will help you find the best solution for your storage environment. Learn about evaluating:

- *Affordability*
- *Ease of Implementation*
- *Virtualization-Enabled Client Transparency*
- *And more!*

Maximize your storage environment
Download this FREE pocket guide at

windowsitpro.com/go/Top10DataMigrationFeatures

Featured resource brought to you by Windows IT Pro Online

Windows IT Pro

Exchange SharePoint

INSIGHTS FROM THE INDUSTRY

Exchange 2010: Problems, Problems, Problems

Microsoft released the first public beta for Microsoft Exchange Server 2010 in April. The beta has received a great deal of web traffic in news stories, blogs, and forums. Exchange Server administrators have weighed in with their thoughts about what they see in this latest version, in some cases praising new features or functionality but in many others voicing some significant and valid criticisms.

One of the biggest complaints I've seen so far about Exchange 2010 is that it seems to be coming too soon on the heels of Exchange 2007. If Microsoft meets its goal of releasing the final version of Exchange 2010 by the end of this year, it will be three years between the two versions, which is the release cycle the company typically tries to maintain. However, that doesn't mean it's been three years since everyone moved to Exchange 2007—that is, those that have moved and aren't still using Exchange 2003.

With mainstream support of Exchange 2003 coming to an end around the time of the Exchange 2010 beta, many organizations undoubtedly decided only in recent months to upgrade to Exchange 2007. And many companies that might have wanted an early adoption probably had to delay any move to Exchange 2007 because of the additional expense of upgrading to 64-bit hardware. Naturally, for the Exchange developers and the true early adopters, three years seems like plenty of time for Exchange 2007 to have worn in like a comfortable shoe, but the reality is that most administrators are still trying to make that shoe fit.

Another Exchange 2010 problem that's causing administrators concern is the fact that there's no in-place upgrade option—even if you're already on Exchange 2007. That situation made sense with the last version because of the necessary hardware upgrade, but what's going on this time? Jørn Stoveland, a reader on the Exchange team blog, commented, "Small companies often don't have the budget to purchase additional hardware. I thought that the migration from 2003 to 2007 was a one-timer because of the transition to 64-bit OS. I hope there is time to reconsider the upgrade options here."

Tony Redmond, in response to a reader comment on his article, "A First Look at Exchange 2010," addressed this point. "Microsoft hasn't forgotten the upgrade option," Redmond wrote. "They just learned from Exchange 2003 how difficult it is to engineer reliable upgrades for all of the circumstances that exist in installations around the world and they learned from Exchange 2007 how smoothly deployments can go when you build servers from scratch."

As true as Redmond's statement might be, it's no consolation for businesses that are already struggling because of the economy. You have to weigh the potential competitive advantage of moving to the newest technology against the actual costs of doing so. My guess is that right now that's going to be a major stumbling block for a lot of organizations—as long as the messaging infrastructure they currently have in place is functioning adequately, beta testing might be all anyone is looking to do.

Unfortunately, even beta testing Exchange 2010 isn't without problems. Here are some of the other common complaints I've seen about the Exchange 2010 beta:

- No 32-bit trial version is currently available, as there was for Exchange 2007.
- Exchange 2010 runs only on Windows Server 2008, meaning a potential dual-upgrade scenario.
- Local continuous replication (LCR) is gone, leading many to feel that Exchange 2010 is aimed only at enterprises, while Microsoft expects small-to-midsized businesses (SMBs) to move to its hosted Exchange services.

Are these all the problems with Exchange 2010? Probably not; I'm sure you've seen others, or experienced them if you're currently testing the beta. And it is, after all, still an early beta; technological problems as well as simply adjusting to the newness and changes are to be expected. I do think it's important that Exchange administrators continue to raise their concerns and let Microsoft know how they feel about these developments.

But let's not forget that there are a lot of exciting new features to look forward to as well in Exchange 2010. What's important, though, is that Microsoft develops a product with the features that administrators need to better do their jobs. Let's hope that's what Exchange 2010 finally delivers.

—B.K. Winstead

InstantDoc ID 102022

Rotary International Implements Website with SharePoint

While SharePoint is typically used as an internal or external document management program, it also can be used as a customer-facing website. Rotary International, the largest privately-funded nonprofit organization, has achieved great success with Microsoft Office SharePoint Server (MOSS) 2007.

The Implementation

Rotary's website, www.rotary.org, was initially developed with static HTML pages. The site suffered from slow performance and was rarely updated with fresh content, due to the hassle of doing so. Additionally, Rotary had plans for a more robust members-only section of the site that the old site was holding back.

"Our old website was on a single server using static HTML pages, running on just a small Linux box. It wasn't very interactive—wasn't very dynamic. If you've seen the old static HTML pages, it provided basic information but it was starting to look a big aged," said Jeremy Contin, manager of the information department for Rotary International. "The organization decided it was time to investigate into new possibilities. We wanted the site to provide better services and build it up to the point where we could start providing specialized information to our members."

One of the other reasons Rotary selected SharePoint was because Microsoft had close integration with F5, provider of the **BIG-IP Local Traffic Manager 3400,** the load balancing tool that Rotary is using now. "One of the things that helped with the decision in choosing SharePoint was the close integration with F5 and Microsoft. Both sides were willing to work together to ensure we got the best performance possible," Contin said.

Why SharePoint?

Rotary is hosted in nine different languages, and SharePoint greatly increases the efficiency of getting all the translations posted on the site. "We can write an article, hand it over to our translators, and pull some translations directly to the website when they're done with it," Contin said.

Granted, transforming SharePoint into a multi-purpose, clean-cut website was a challenge. The main struggles for Rotary were learning the system and getting the

"It wasn't the easiest time in the world to customize SharePoint. When you look at the site, it looks nothing at all like the default SharePoint. And that was part of our goal."

—Jeremy Contin, manager of the information department for Rotary International

design to the point where it wasn't obvious that SharePoint was used. Altogether, the process from deciding to use SharePoint to implementing the site took 6–9 months.

"It wasn't the easiest time in the world to customize SharePoint. When you look at the site, it looks nothing at all like the default SharePoint. And that was part of our goal—we didn't want you to go on the site and know it was SharePoint right away," Contin said. "So we spent a lot of time manipulating the system. The other problem early on was performance. It took a lot of time to get it tuned so that it moved this quickly. There's always bugs in code the first time around, no matter how hard you try. It took us awhile to resolve all those things."

Successful Implementation

Since implementing the site, Rotary has freed up server processing usage by as much as 20 percent. But of course, many of the benefits of the new site cannot be quantified in numbers: happier customers, less stress for employees, easier management of content and administering of the site, and the peace of mind that the site is prepared to move forward as Rotary does, rather than slowing down the organization's goals.

"In general our customer base has been happy with the new site. They like the fact that it's running quicker and that it's updated with new content quicker," Contin said. "The site is pretty up on the new technology even though it doesn't look like it. It's not very flashy, but it works."

Think using SharePoint for a customer-facing website might be for you? Visit Microsoft's SharePoint site at www.microsoft.com/Sharepoint/default.mspx to learn more. For additional resources, you can subscribe to our Office & SharePoint newsletter at windowsitpro.com/email.

—Brian Reinholz

InstantDoc ID 101989

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Exchange & Outlook UPDATE*
- *Scripting Central*
- Security UPDATE
- SQL Server Magazine UPDATE
- *ToTheSharePoint Newsletter*
- *WindowsDevPro UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro*, via the new, banner-free VIP Web site.
www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEB SITES

WindowsDev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at WindowsDevPro.com, where IT pros creatively and proactively drive business value through technology.
www.windowsdevpro.com

Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.officesharepointpro.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Regional Forums: We've introduced regional areas in our online forums, allowing IT user group leaders and other readers interested in meeting locally to more easily communicate with each other. Visit our forums at www.windowsitpro.com/forums and scroll down to see the new regional forums.

Windows IT Pro

by Jason Bovberg

5 More Time-Wasting, Productivity-Trashing Online Games

We got a great response to our July 2008 listing of five time-wasting online games, so we've come up with five more that will consume your work hours.

5. **Crush the Castle**
(armorgames.com/play/3614/crush-the-castle)

4. **Exorbis 2**
(www.kongregate.com/games/editundo/exorbis-2)

3. **Civiballs**
(armorgames.com/play/3434/civiballs)

2. **Robokill**
(www.rocksolidarcade.com/games/robokill/)

1. **GemCraft**
(armorgames.com/play/1716/gemcraft)

User Moment of the Month

"At the IS service desk where I work, I received an email message from one of my supervisors that read, 'I have this symbol, a backwards P with two legs, and I can't get rid of it. It causes dots between words, and when I hit Enter, I get more of the backwards Ps. Help!' When I controlled my laughter, I calmly explained to the supervisor that she had enabled paragraph marks in Microsoft Word."

—Tony

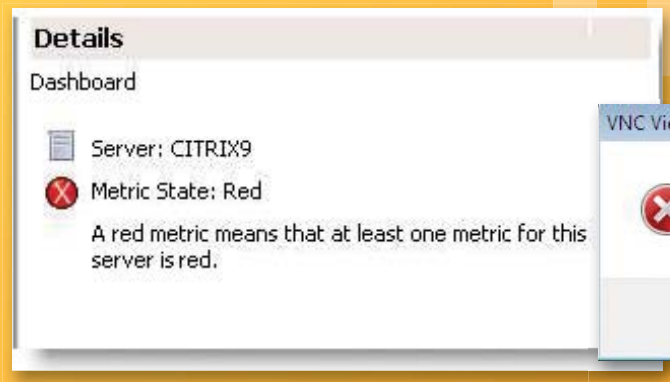
Tech Gadget of the Month

Our favorite press release this month touts the Pogo Stylus ($14.95), an iPhone-compatible stylus that simplifies iPhone navigation for women with long fingernails ("acrylic or natural"). Many such women "have experienced difficulty [using] the iPhone's touch-screen interface. The capacitive screen was designed to only respond to the electrical charge of your fingertip—so nails won't work."

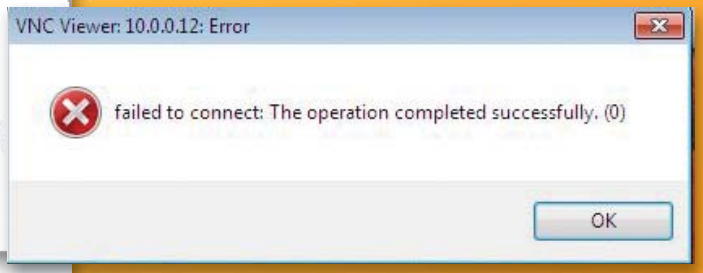
The aluminum body of the stylus acts as a bridge, transferring the electrical charge from your hand directly to the screen. "Plus, it comes in four hot colors: cranberry, silver, black, and gunmetal." For more information, check out the Ten One Design website (www.tenonedesign.com).

SEND US YOUR INDUSTRY HUMOR!

Email your industry humor, scandalous rumors, funny screenshots, favorite end-user moments, and IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a gift.



Seeing red



Success is not an option

July 2009 issue no. 179, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.

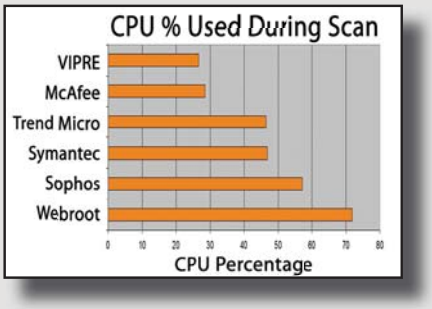
Kiss your antivirus bloatware goodbye

Special Competitive Upgrade Price: $10 per seat!

TEST DRIVE VIPRE® ENTERPRISE

Next Generation of Total Malware Protection

The configurable Command Center puts all the information you need in one place. Manage individual agents, quarantines, threats, and more.



How does your current software compare? VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Sunbelt Software

Until now, antivirus engines have been Frankensteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise is a revolutionary new approach. It's built from scratch as the all-in-one antivirus, antispyware, anti-rootkit solution that gives you complete endpoint malware protection ***without hogging resources!*** It's fast, powerful, and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Low $10 per seat pricing to save you money.

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

Curious? Download your FREE copy of VIPRE Enterprise and give it a test drive.

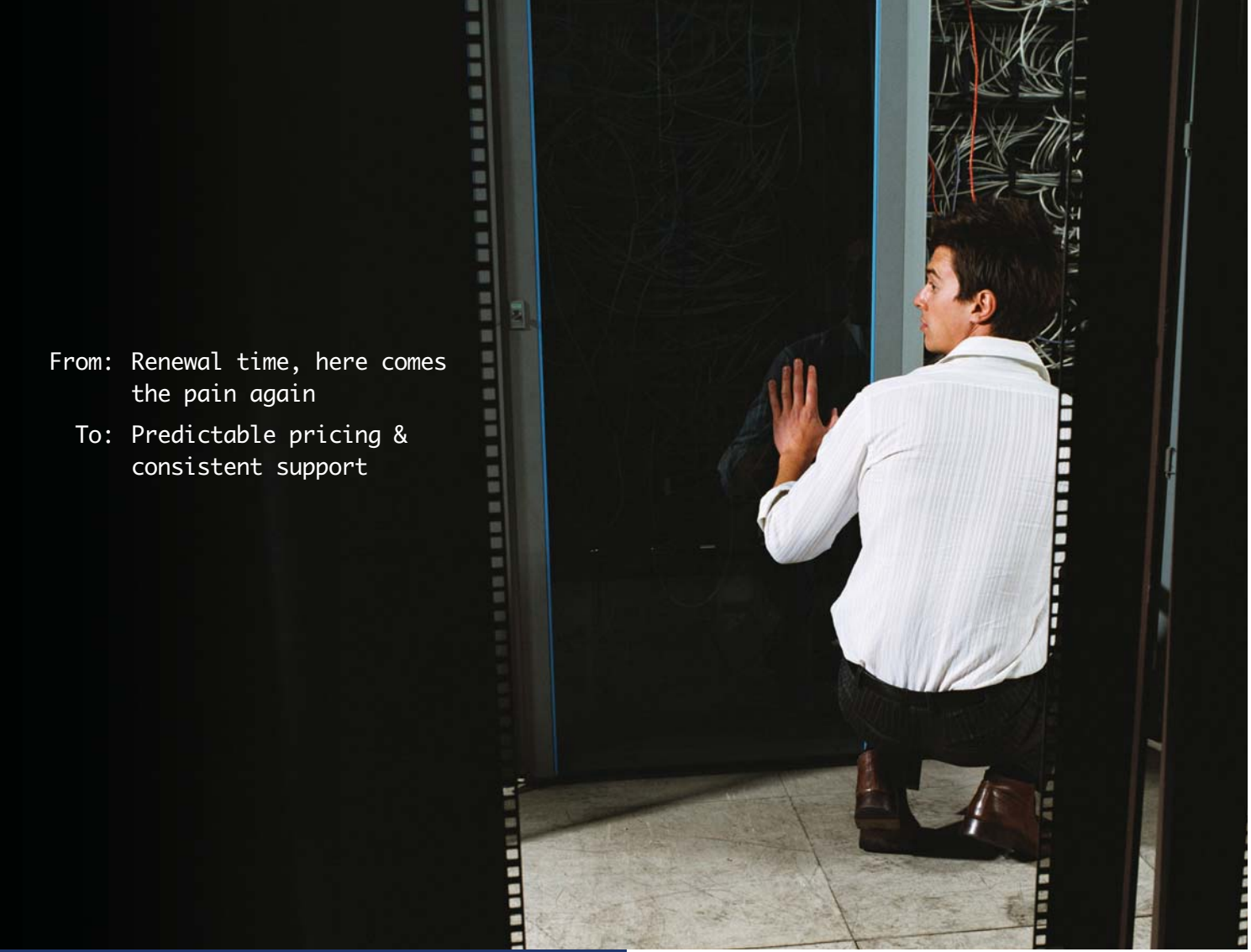
When you compare VIPRE Enterprise to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though.You can get VIPRE Enterprise at our competitive upgrade price of **only $10 per seat!**

Download VIPRE Enterprise today and get your own home version of VIPRE to keep FREE as our gift to you!

Download now: www.TestDriveVipre.com

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com

New licenses are available for $10/seat up to 500 seats, minimum 10 seats. For customers with over 500 seats, please call for special pricing. Available for a limited time and subject to change without notice. See website for more details.



NO-NONSENSE WEB FILTERING

That's what you'll get when you switch to iPrism from St Bernard – the award-winning web filter that's easier in every way, and less expensive to own.

iPrism is changing the way companies and schools everywhere handle their web filtering. With blazing throughput speeds up to 100+ Mbps, anti-virus protection and seamless XenApp and Active Directory integration, iPrism is the appliance-based solution of choice for customers and institutions of any size.

Find out more about the easiest-to-deploy, most highly rated web filtering solution ever – the industry's ONLY Citrix-ready web filtering appliance.

Call 1.800.782.3762 or go to www.SwitchToiPrism.com/flip

ST BERNARD

FLIP THE SWITCH

Get your FREE iPrism® Switch Kit today:

FREE 30-day onsite evaluation
that can be deployed without any client or network changes

FREE enhanced technical support
for setting up matching policies, reports & alerts based on your current settings

INCENTIVE PRICING & A FREE T-SHIRT
just for watching a live demo

iPrism® h-Series, the world's #1 Web Filtering appliance.